University of Kentucky
UKnowledge

Theses and Dissertations--Education Sciences | College of Education

2023

The Protection of Student Data Privacy in Wisconsin School Board Policies

Curtis Clyde Rees
University of Kentucky, curtrees@gmail.com
Digital Object Identifier: https://doi.org/10.13023/etd.2023.071

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Recommended Citation

Rees, Curtis Clyde, "The Protection of Student Data Privacy in Wisconsin School Board Policies" (2023). *Theses and Dissertations--Education Sciences*. 123.
https://uknowledge.uky.edu/edsc_etds/123

This Doctoral Dissertation is brought to you for free and open access by the College of Education at UKnowledge. It has been accepted for inclusion in Theses and Dissertations--Education Sciences by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Curtis Clyde Rees, Student

Dr. Justin Bathon, Major Professor

Dr. John Nash, Director of Graduate Studies

THE PROTECTION OF STUDENT DATA PRIVACY IN WISCONSIN SCHOOL BOARD POLICIES

DISSERTATION

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the College of Education at the University of Kentucky

By
Curtis Clyde Rees

La Crosse, Wisconsin

Director: Dr. Justin Bathon, Associate Professor of Education

2023

Copyright © Curtis Clyde Rees 2023

ABSTRACT OF DISSERTATION

THE PROTECTION OF STUDENT DATA PRIVACY IN
WISCONSIN SCHOOL BOARD POLICIES

American schools have increasingly adopted technology resources to fulfill their educational obligations. These tools are for instruction, communication, and storing and analyzing student information. Student data can be directory information, enrollment records, achievement data, and student-created products. This increased utilization began with the passage of No Child Left Behind in 2001, and the COVID-19 pandemic led to more educational technology use of student data. Districts turned to third-party vendors for assistance with data systems and virtual learning resources. Before, during, and after the pandemic, stakeholders were concerned about information security and the students' privacy.

School leaders looked to federal regulations to ensure appropriate and legal practices for student data use. The Family and Educational Rights and Privacy Act (FERPA) was implemented in 1974, and the growth of educational technology and digitization of student information has moved beyond the original guidance of the regulation. District leaders also looked to state laws, but Wisconsin statutes provide little guidance. These leaders rely on their local board policies to ensure they benefit from educational technology while protecting the privacy of their students.

I utilized the methodological approach of document analysis and the contextual integrity privacy framework to understand how Wisconsin districts address student data privacy in local board policies. In addition, I examined how federal regulations are addressed and the role of leadership in policy implementation.

Findings from this study indicate differences for districts using a policy consultation service. These policies address federal regulations and account for the use of data by modern educational technology. The leadership activities required for student data privacy align with previous research for effective educational leadership. These findings show the need for local policies to address federal regulations for student privacy in the context of educational technology utilization.

KEYWORDS: Student Data, Privacy, Board Policy, Wisconsin, Contextual Integrity

Curtis Clyde Rees_____

April 6, 2023_____

STUDENT DATA PRIVACY IN WISCONSIN SCHOOL BOARD POLICIES

By

Curtis Clyde Rees

Dr. Justin Bathon
Director of Dissertation

Dr. John Nash
Director of Graduate Studies

4/6/2023
Date

ACKNOWLEDGEMENTS

I am grateful for the support and encouragement I received while completing this doctoral program, especially during the dissertation phase of my studies. My wife, Dr. Keely Rees, was a continuous source of wisdom, comfort, and the needed push to finish. My children Gavin and Harper are the best dissertation cheerleaders I could imagine.

From preschool to Ph.D., my parents Curtis and Dianne have always been there for me. Thank you to my brother, Dr. Carter Rees, for the many texts and phone calls to discuss research. My brother Clay is a model for tenacity and focus when faced with challenges.

Dr. Justin Bathon has been my chair for a long time. He has been a source of strength and encouragement throughout the program, and I cannot thank him enough for his continued support to help get me to the end. I am grateful for my committee members and their wise counsel to make my study meaningful – Dr. Gerry Swan, Dr. Mary John O'Hair, and Dr. Amanda Potterton. Thank you, UK EDL faculty, past and present, for giving me this opportunity. I thank Dr. John Nash, Dr. Tricia Browne-Ferrigno, Dr. Beth Rous, Dr. Jayson Richardson, and Dr. Scott McLeod.

I appreciate my cohort mates and friends from the early days of the UKSTL program. Thank you to Dr. Todd Norton, Dr. Tyler Gayheart, Dr. Todd Hurst, Dr. Ericka Hollis, Dr. Jill Janes, Dr. Dana Watts, Dr. Joshua Marsh, and Robert Appino. You all made this fun.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Starting in the early years of the 21st century, schools in the United States have increasingly adopted technology tools and resources to fulfill their obligations to students, staff, and their communities. These tools are used for instruction, communication, and storing and analyzing their students' information (Davies & West, 2014, p. 136). This student data can be in the form of directory information, enrollment records, achievement data, and the students' products (Krueger & Moore, 2015; Trainor, 2015).

Since the passage of No Child Left Behind in 2001, states and schools have been required to participate in longitudinal data systems as part of a school accountability movement where student data was used for evaluating the effectiveness of districts, schools, and educators. Most districts did not have the resources to develop or maintain their own data systems, so they turned to private off-site vendors or cloud services for these data systems (Molnar & Boninger, 2015; Reidenberg et al., 2013). These cloud service vendors had advantages for schools as they could hold large amounts of student data, maintain security issues, and easily share information with learning analysts (Weber, 2016). However, as soon as schools began working with these third-party vendors, parents, educators, and lawmakers voiced concerns about the security of student information, who had access to this data, and the privacy of the students (Bathon, 2013a).

The use of educational technology quickly accelerated due to the Coronavirus (COVID-19) pandemic, which began to impact the United States in the spring of 2020. At that time, 77% of public schools reported moving some instruction to online formats (Berger et al., 2022). The pandemic's impact on education continued into the following school year, as 62% of schools reported that their students would begin the year in online formats (Roche, 2020). The COVID-

19 pandemic negatively impacted almost all aspects of American education, including the concern for the privacy and security of student information created and used in online services.

As school leaders looked to federal regulations regarding student information in the digital world, there was a realization that there was no universal legislation for electronic student records. The Family and Educational Rights and Privacy Act (FERPA) was enacted in 1974, and the growth of educational technology and student records moved beyond the language in that legislation, so there was no clear guide for maintaining the safekeeping and use of electronic student information. Districts and superintendents had to look to their local policies or state legislation, if addressed by their state, to ensure they could benefit from the new educational technology while still protecting the privacy of their students. This intersection of local policies, federal regulations, and educational technology formed the basis of this study.

In this study, I sought to examine the concept of privacy and how school board policies in Wisconsin address it as schools use student information through educational technology. I analyzed school board policies from Wisconsin public schools using the qualitative research method document analysis. Through this analysis, I hoped to understand how districts addressed protecting student information and students' privacy. This study examines how these board policies address the federal regulation requirements of student records and how boards address privacy in general through the privacy concept of *contextual integrity*, an established framework for exploring privacy and information flow (Nissenbaum, 2010). Additionally, this research explores the role of school leaders in implementing and managing student data privacy policies.

In this first chapter, I will establish the context and rationale for the development of this study. First, I provide background to the issue before explaining my approach to the concept of privacy in the context of digital student information used by modern educational technologies. I

will then present the research questions that focus the study. Finally, I detail the significance of the study and explain the study's limitations and assumptions.

Background of the Problem

The frequent attempts by researchers to define privacy have led to a variety of results (Nissenbaum, 2010; Solove, 2002, 2006, 2008; Vasalou et al., 2015). The challenge to develop a universally accepted and concise definition is due to the varying players, environments, eras, legal settings, business applications, and technological developments (Vasalou et al., 2015). Previous attempts to define privacy have included the right to be let alone, limiting access to the self, secrecy, control of personal information, personhood, and intimacy (Solove, 2008; Warren & Brandeis, 1890). Researchers, philosophers, and lawmakers have seen privacy as a right, a foundation for personal freedom, and a condition necessary for trust, social progress, and the development of relationships (Nissenbaum, 2010). Other researchers have examined privacy through the issues or harms that result from the intrusion on privacy. Technological advancements with information collection, storage, and analysis have led to privacy harms, and a body of research is dedicated to privacy in our digitally connected reality (Nissenbaum, 2010; Ohm, 2014; Solove, 2008; Tavani, 2008).

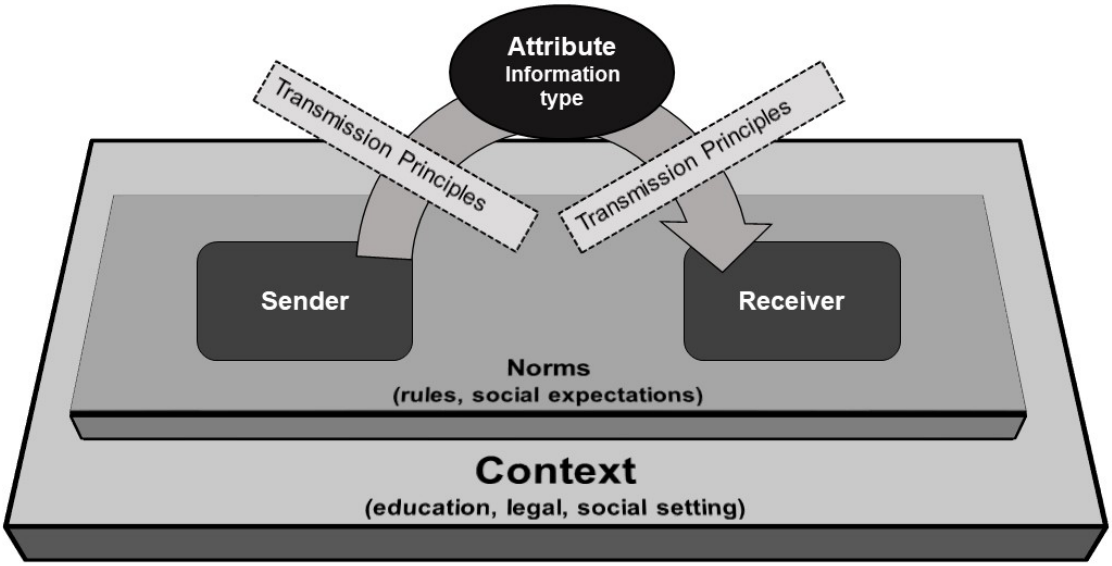
Contextual Integrity

For this study, I have chosen Nissenbaum's (2010) *contextual integrity* (CI) framework to understand how board policies address privacy. I chose this framework because it was developed to address the issues and concerns arising during the age of connected technologies, which lead to the production, collection, analysis, and sharing of digital personal information. Nissenbaum's work recognizes the changing nature of technology amidst various contexts, such as health care, the legal system, and education. Nissenbaum explains how the control of personal information

occurs within different systems and is dependent upon the environment's prevailing norms and rules. The contextual integrity framework is responsive to historical, cultural, and geographic settings. The norms about information flow can change over time and within different settings. This framework seems appropriate for analyzing privacy rules and expectations within school systems as those contexts can vary widely from community to community.

The CI concept is based on the privacy issues which may occur within different social structures or contexts. Within a particular context, the flow of information involves a sender, a recipient, and the subject of the information being shared (Figure 1). This flow of information is influenced and judged by the norms from that specific context. The norms can be formal regulations and laws regarding information or moral and social expectations. Key features of the framework are contexts, actors, attributes, and transmission principles (Nissenbaum, 2010). Contexts are the environments in which information is shared or withheld. Actors are the people within the contexts who produce, share, receive, and use information. Attributes are the different types or descriptions of information that may or may not be transmitted among actors. Transmission principles are the conditions in which information is or is not shared. These concepts of the CI framework work together to determine if there is integrity within the system for the flow of information. The system's integrity is evident when information is shared according to the norms of the context.

Figure 1 - Contextual Integrity Flow of Information



Note. Information may flow from a sender to a receiver, and this process is influenced by transmission principles of the norms of the context in which the flow exists.

Privacy Law in the United States

This study begins with examining privacy law, past and present, in the United States to understand the concern and need for regulations that affect student data use today. While the U.S. Constitution does not use the term *privacy*, it does address different privacy issues (Schwartz, 2013; Solove, 2016). The First, Third, Fourth, and Fifth Amendments are the bills that have primarily determined privacy rights in the country. While not a law, Brandeis and Warren's (1890) privacy concept of "the right to be let alone" led to a national debate and subsequent legislation defining and protecting an individual's right to privacy (Bratman, 2002). As technology changed in the country, so did privacy issues with the proliferation of newspapers and developments with the telegraph, mail system, telephone, cameras, and other electronic communication devices and methods. Several laws were passed at the federal level to address privacy harms as the result of these technologies. The Federal Communications Act was enacted

in 1934 and the Freedom of Information Act in 1966. The Fair Information Practices Principles were written and adopted in 1973 and were used as a framework for a variety of other regulations and practices. The Health Insurance Portability Accountability Act of 1996 was the first federal legislation to address the privacy of health information (Solove, 2016).

Four pieces of legislation address the use of digital information from children. The Children's Internet Protection Act (CIPA) was enacted in 2000 in response to concerns about children accessing harmful and obscene content on the internet. The Family and Educational Rights and Privacy Act (FERPA) was enacted in 1974 to regulate student information use and sharing in education settings. Its primary purpose is to protect students' educational records in school. Several updates and regulatory changes have altered FERPA since its inception, but there are still several criticisms of the law as it does not protect student information in all contexts. The Protection of Pupil Rights Amendment (PPRA) was enacted in 1974 with several significant updates since it became law. PPRA primarily regulates the collection of sensitive personal information from students in surveys, evaluations, and research. The Children's Online Privacy Protection Act (COPPA) became law in 1998 and governs information collected from children. COPPA mainly regulates private companies and websites that market their services to children under 13 and requires parental permission before child users can disclose personal information (Federal Trade Commission, 2012). Each of these four laws regulates privacy in different manners and contexts. Despite their application, there are still gaps in protecting student information in online environments.

In the state of Wisconsin, there is no state legislation explicitly addressing the protection and privacy of student data. State statute 118.125 gives general guidelines for the confidentiality and maintenance of student records. Then it stipulates that local school boards should adopt

policies for the appropriate storage and disclosure of student information. The 2019 State Student Privacy Report Card gave Wisconsin and ten other states the grade of F for not having significant state legislation addressing student data privacy (Strickland, 2019).

Educational Technology Growth

The technology schools use vastly changed from systems that store data on local devices to cloud-based services where third-party vendors store the information on servers far from the actual buildings where students attend school (Reidenberg et al., 2013; Takabi et al., 2010). This technology changes quickly, which can lead to concern for the maintenance of the security of student data. When the data was stored locally, responsibility for privacy maintenance rested with local school district employees. That responsibility is now shared with the people and organizations managing cloud computing services.

In addition to the concerns about where the data is stored, there are privacy issues with how easily data can be shared (Bathon, 2013a; Takabi et al., 2010). Data sharing within technology resources can benefit students as they move up grade levels or from one education institution to another. Educators benefit from this portable data as they can better understand the needs of students. However, the technologies that enable this intentional beneficial sharing can also lead to privacy concerns. There were privacy concerns as new technologies were being developed and used in the early years of this century, and those concerns were still evident during and after the COVID pandemic. These digital tools can also allow vendors access to the data, and they may use it for unwanted marketing purposes. The same features of these tools that enable intentional sharing among legitimate users could also contribute to user errors that would cause accidental sharing of student data. The challenge for educational leaders, as technology-

centered learning becomes more common, is to design methods and create policies to use these digital resources while safeguarding student data privacy effectively.

School Board Policy

Wisconsin state statutes task local school boards with creating and adopting policies to address student records, including digital student information (Wis. Stat. § 118.125(2)). Wisconsin school boards are comprised of non-partisan elected members responsible for providing the fiscal and academic foundation for the students in the district. Most of the board's work is to develop policies to guide the work of the educators on staff. Since most board members are not professional educators, they rely on a partnership with the district's superintendent and other school leaders to ensure policies are in place to outline the procedures and practices used to meet the goals of the district and the needs of the students and school community.

Superintendent Leadership

Second only to classroom instruction, school leadership is the most significant factor contributing to student learning success (Leithwood et al., 2010). Superintendents work with school boards to develop policies and work with the district employees to ensure they follow the procedures and practices resulting from the policies. School leadership styles and activities have been the topic of decades of research. Effective leaders develop a vision, set clear expectations, understand the change process, take appropriate risks, and are learners themselves (Richardson et al., 2015; Seashore Louis et al., 2010; Waters et al., 2003). These same dispositions are true for effective leadership with technology initiatives. In addition to the descriptors of general school leadership mentioned above, leadership for effective technology use also focuses on

infrastructure, effective communication, and providing professional development for themselves and the rest of the district staff.

Statement of the Problem

The increased use of digital tools in schools, the need to maintain students' privacy, and the data they produce have brought forth new issues for school leaders. As school districts adopt new technologies for instruction, learning, data storage, and analysis, education leaders must also balance the need to protect the information essential for understanding their students' achievement and the effectiveness of their instructors and programs. While a body of literature discusses the nature of general privacy rights and regulations for student information in schools, there is a lack of empirical research examining how districts interpret and implement the regulations through board policies. As there is no specific state legislation in Wisconsin addressing student data privacy, this study will help illustrate how districts currently address the federal regulations in place. This research will also examine how board policies specify the leadership and management of privacy practices.

Purpose of the Study

The study aims to examine Wisconsin P-12 school board policies to understand how those policies address the privacy of student information. To accomplish this, I developed three research questions. I used the document analysis methodology to analyze these board policies through the lens of Nissenbaum's (2010) concept of *contextual integrity* in understanding privacy.

Research Questions

I used a qualitative approach to this study and sought to understand the policies and procedures of data protection using document analysis. I followed three research questions to

guide the inquiry.

1) How is student data privacy protection addressed in the student records sections of school board policies in public school districts in CESA 4 in Wisconsin?
2) How do these local policies address federal student privacy obligations?
3) Who do these policies task with leading and managing the implementation of student data privacy policy?

I used research question one to gain an overall understanding of how school districts describe their procedures for addressing the use of student information. Research question two is used to understand how district policies specifically address the federal regulations of FERPA, COPPA, and PPRA. Finally, the third research question helps explain how leaders implement and execute student data privacy policies.

I have employed document analysis to address these research questions, drawing on Bowen's (2009) and Prior's (2003) work. This approach requires that I examine the board policy books of the selected school districts with a focus on the policies which address record keeping and sharing of student information. To preserve the intended meaning and context of these policy documents, they were collected in their entirety (Hatch, 2002; Merriam, 2009; Prior, 2003). I focused my analysis on the contents within the student records section of each of the policy books. To derive meaning from these policy documents, I followed the work of several methodological scholars (Bowen, 2009; Creswell, 2009; Hatch, 2002; Merriam, 2009; Owen, 2014) by consolidating and organizing smaller pieces of data to help understand larger themes from the information in these school policy documents.

Since the contextual integrity privacy framework guides this research, I used the typological analysis approach Hatch (2002) described. In my initial reviews of the policy books,

I tagged passages related to Nissenbaum's (2010) concepts of *context, actors, attributes,* and *transmission principles*. I also used the three federal regulations as typological categories during coding. These regulations were the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children's Online Privacy Protection Act (COPPA). The analysis is an iterative process, as I reviewed each document several times, looking for each of the typologies mentioned above. As Hatch (2002) recommended, I only looked for one typology at a time, tagging all those passages before moving on to the next round of review with a different category in mind.

After these initial searches and rounds of coding and tagging the passages according to the typologies mentioned above, I looked for patterns, themes, and relationships (Hatch, 2002). I used memo writing to track my hunches and interpretations as I looked for these themes and relationships. In addition, I frequently referred back to the literature on contextual integrity and federal regulations to see if these emergent themes made sense with those frameworks.

Significance of the Study

Schools will continue to rely on educational technology tools for instruction, communication, information collection, storage, and analysis. These technologies will likely continue to develop faster than laws and board policies adapt to address these tools' new advantages and challenges. Student information will continue to be a vital component of these digital resources. Protecting student data will still be a concern for educators, especially for leaders who promote using these tools and work with other school leaders to develop appropriate privacy policies. There appears to be no imminent federal or Wisconsin legislation addressing student data privacy and protection, so board policies will continue to be a primary guide for using educational technology and protecting student records and other information.

The professional significance of this study lies in the possibility of doing three things. First, it will serve to understand better how Wisconsin school board policies currently address student privacy issues through Nissenbaum's framework of contextual integrity. The second significance is the potential to understand how Wisconsin board policies address the three federal regulations (FERPA, COPPA, and PPRA) that are significant for using student records in digital environments. Finally, this study provides insight into school leaders' roles in implementing board policies that address student data privacy. Additionally, this study has the potential to extend the research methodology employed. Document analysis has been used to understand many sources of information. Still, few studies have used the method to examine student privacy issues within digital contexts.

Assumptions and Limitations

Document analysis is a research methodology that relies on the researcher to find and label various information within sources to ascribe meaning and intent. As such, others might interpret this information differently than I have. My primary source of information is the board policies of school districts. Still, other district documents likely address the topic of student data privacy but are not within the policy books. These additional sources could bring additional information to understanding the language and intent within the policies.

I also recognize that board policies show the intent of school board members to guide the work of other district employees. However, these policy guidelines may not be known or followed by district employees, so there are likely variances of practice significantly different than what is found in the policies.

Finally, my interest in data privacy and technology use came from my experience working as a school administrator in a public school district. In that role, I frequently worked

with other administrators and school personnel who viewed the advantages of educational technology with more caution than I did. They had more concerns about data privacy issues based on their interpretation of privacy laws. I was also familiar with the federal regulations, but there were times when the vagaries of the laws led to their hesitance to use new technologies, and I was apt to move on since the regulations did not clearly address the issue.

Conclusion

In this study, I sought to examine an area that continues to grow significantly as schools rely more on digital technologies for instruction, learning, record-keeping, and data analysis. I believe I have brought forth new findings and questions regarding how Wisconsin board policies address student information privacy. In the next chapter, I present an overview of the scholarship regarding the concept of privacy, especially concerning student privacy in the digitally connected world. Next, I discuss the theoretical approach guiding this study and describe how it frames my understanding of how school board policies attempt to safeguard their students' data. I also describe the role school board policies play in guiding the procedures and practices of school personnel. Finally, I discuss the role of the superintendent as they work with local school boards to create and adopt policies that guide the work of the educators in the district.

CHAPTER 2: REVIEW OF LITERATURE

This study aims to understand how P-12 school board policies in Wisconsin address student data privacy and how these policies meet the requirements of federal laws regulating student records. This literature review begins by examining general concepts and attempts to define privacy. Next, it summarizes research on conceptual frameworks regarding privacy and explores in more detail Nissenbaum's framework of *contextual integrity.* Next is an examination of federal regulations regarding privacy as they relate to students in schools. The most applicable regulations for this study are the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Protection of Pupil Rights Amendment (PPRA). The literature review also gives the background for the organization of public schools in Wisconsin, how state legislation addresses student data privacy, and how the state's Department of Public Instruction guides schools in matters concerning student records.

The review then outlines the growth of technology use in schools from the early years of this century after the enactment of No Child Left Behind through the COVID pandemic. Next, the literature review addresses how technology use has led to concerns from parents, school personnel, and lawmakers about the privacy and security of student information. There is then a review of research on leadership within schools and how the work of superintendents and school boards impacts student learning. Research is then shared about the relationship between school boards and superintendents and how they develop and adopt policies to guide the work of the rest of the school personnel. The final part of this literature review shows what research says about effective school leadership and how those skills apply to leading technology efforts within the school district.

Definitions of Privacy

Privacy is a vast concept and has been difficult for researchers to define concisely (Nissenbaum, 2010; Solove, 2006, 2008; Vasalou et al., 2015). Nissenbaum (2010) states:

> Attempts to define it have been notoriously controversial and have been accused of vagueness and internal inconsistency--of being overly inclusive, excessively narrow, or insufficiently distinct from other value concepts (p. 2).

The concept of privacy has been challenging to understand in simple and universally accepted terms because of the involvement of varying players, social environments, legal contexts, business applications, and technological advancements (Vasalou et al., 2015). The attempts to understand and define the general concept of privacy have become especially relevant with the rise of technological innovations which produce large quantities of data and artificial intelligence tools used to analyze and make sense of it. Educational practitioners desire to appropriately use new learning technologies while maintaining the security of the data they use and the privacy of the persons who have produced the information.

Solove's Examination of Privacy Definitions

Several researchers have attempted to understand privacy by examining previous work on the concept. Solove (2008) categorized the theories of privacy into six categories:

- the right to be let alone
- limited access to self
- secrecy
- control over personal information
- personhood
- intimacy

Warren and Brandeis Definition

The concept of the *right to be let alone* is from the work of legal scholars Samuel Warren and Louis Brandeis (1890) as they wrote in the Harvard Law Review about how the developing technologies of photography and the proliferation of newspapers threatened the privacy of individuals at the end of the 19th century. New cameras invented by Kodak Eastman made it easy for laypeople to take photographs. The newspaper industry at the time was sensationalistic and published many stories and photos about the personal lives of citizens. It was not solely an issue of whether the news business profited from publishing information about individuals but focused on the importance of "the peace of mind or the relief afforded by the ability to prevent any publication at all" (Warren & Brandeis, 1890, p. 200). They posited that individuals have the right of "determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others" (p. 198). Soon after the publication of their article, courts and lawmakers began to see privacy as a right (Solove, 2008). Westin (1970) built on this privacy concept to say that individuals have the right to freedom from surveillance by others.

Limiting Access to Self

Like the right to be let alone, the *limitation of the access to self* is an idea that the individual can decide what information is known to others (Solove, 2008). This concept of privacy is a choice of who has access to the self. Godkin (1880) described it as the "right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be subject of public observation and discussion" (p. 786). Individuals have the choice to limit what others can know about themselves.

Secrecy

Secrecy is another common interpretation of privacy and is the intentional concealment of facts that might be harmful if publicly known or used by others to the disadvantage of the secret holder (Costas & Grey, 2014; Slepian et al., 2017; Solove, 2008). This notion of privacy sees it as limiting the information that has been intentionally concealed. What is challenging about this view of privacy is that some information considered *secret* is contextual. This information may be intentionally shared with certain people but withheld from others.

Control of Personal Information

Control over personal information is another familiar concept of privacy and is focused on the ability of an individual to determine what personal information is shared about oneself and who can know that information (Bergelson, 2003; Solove, 2008; Westin, 1970). A problem with this narrow definition of privacy is being unable to precisely determine what information is considered personal (Braman, 1989; Schwartz & Solove, 2014).

Intimacy

Some have defined privacy as a form of *intimacy*. Privacy is an essential aspect of individual existence and relationships in which the individual participates (Solove, 2008). A lack of privacy can be detrimental to the development of some human relationships. Rachels (1985) says, "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people" (p. 3). There is information we want to only share with certain other people, which is often an essential part of the relationship. Derlega and Chaikin's (1977) concept of privacy identified how individuals can self-disclose information and control the flow of what is known about themselves as relationships form. This form of privacy is found

in relationships between spouses, romantic partners, or between a patient and a medical provider.

Nissenbaum's Definitions of Privacy

Nissenbaum's (2010) overview of privacy described it in similar ways. It is a "fundamental human right (not merely a preference or an interest)" (p. 9). The research shows that privacy is a form of self-expression and ownership, the right to be let alone, a foundation for personal autonomy and freedom, and a condition necessary for "trust, friendship, creativity, and moral autonomy" (p. 9). Nissenbaum cautions that trying to provide an accurate account of privacy can hinder progress toward solving social issues that arise due to conflicts with sharing personal information, no matter the definition of privacy.

Layperson's Definition of Privacy

A study by Vasalou et al. (2015), aptly titled "Privacy as a Fuzzy Concept," examined how lay people define or describe privacy. The study population consisted of more than 300 people of various ages, occupations, and levels of education. No one definition or component was predominant, but the most agreement came from the concepts of *secrets*, *being alone*, *personal space*, and privacy as a *right* or *entitlement*. The descriptors from this study are also found within the varying academic concepts of privacy described previously in this review. While many have tried to describe privacy concisely, there has yet to be a widely accepted definition; as Thomson surmised, "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea about what it is" (1975, p. 1).

Conceptualizations of Privacy

The literature defines privacy in many ways, but it is helpful to view this issue through a conceptual or theoretical framework to understand better and analyze specific privacy policies.

Tavani (2008) examines information-related concepts, and Martin views privacy through *social contract theory*. Solove's (2002, 2006, 2008) concept of privacy posits no singular way to define it theoretically or philosophically. Instead, one should examine privacy through the specific situations and circumstances in which privacy disruptions occur (Solove, 2006). Like Solove's examinations of privacy disruption, Ohm (2014) adds to the literature on understanding privacy by suggesting how to best use big data, including analyzing gaps and vague definitions in current U.S. laws that may lead to data misuse and harm to individuals.

Finally, the privacy concept of *contextual integrity* (CI) from Nissenbaum (2010) is outlined later in this chapter to show the importance of the issue regarding student data privacy. Nissenbaum's *contextual integrity* is a framework for understanding the flow of information among agents who use the information (Barth et al., 2006; Nissenbaum, 2010). This concept emphasizes the expected use of information among the many intricate systems where data flows. Nissenbaum's contextual integrity framework is an appropriate privacy concept for exploring and describing student data privacy in schools.

Information Privacy

Tavani (2008) specifically examined informational privacy through the lens of a variety of theories, concepts, and controversies. Early in American law, privacy was thought of as a physical concept where people had the right to avoid sensory intrusion and be able to place restrictions on bodily interactions with others. This view can be traced back to Warren and Brandeis (1890), who stated that people had the right to be let alone and free from intrusion. One can understand privacy as a decisional concept where one can be free of interference in "personal choices, plans, and decisions" (Tavani, 2008, p. 136). This issue is of particular concern when an individual is making choices in health care, career, marriage, and religious practices. The issue

has also been examined within the more abstract concepts of psychology and mental privacy (Shen, 2013; Wajnerman Paz, 2022). People should be free from interference in their thoughts, personality, and mental well-being, even when the intrusion is not from physical means. Regarding modern technology, these mental intrusions occur when social media comments, communications, and other digital content are threatening, degrading, or disturbing.

Restricted Access and Limited Control

The increased computing power led to an exponential rise in personal information being collected, stored, analyzed, and shared. *Restricted access theory* is undoubtedly relevant to personal information as people strive to have the ability to limit or restrict the amount of their data that others can access. Control theory is a more active approach to information privac*y* when an individual has actual control over information about oneself (Rachels, 1985; Tavani, 2008). The *Restrict Access/Limited Control Theory* (RALC) describes the creation of zones where a person can limit or restrict access to their personal information, depending on the situation and the type of personal information being shared or restricted.

Social Contract Theory

Martin (2012, 2016) has used social contract theory to understand privacy. A social contract approach is situation-dependent and differs from previous static definitions of privacy. Social context theory views of privacy are relativistic as they depend on the current culture, society, and historical context. This view of privacy is also essential to the community in which individuals relate to one another. People develop commonly accepted norms in these communities as they share tasks, values, and goals. As a result, communities develop expectations about privacy and information sharing. As communities and cultures change, so do

expectations for information flow and privacy. A social contract view adds procedural and structural norms to evaluate the other local standards. (Martin, 2012, 2016).

Solove's Concept of Privacy

Solove's work in *Understanding Privacy* (2008) states that one can best understand privacy by looking at the particular conflicts and problems that occur with privacy instead of trying to create a specific or overarching definition. The issue with attempts at a broad definition of privacy is that these general descriptions can be too inclusive of other definitive efforts. This often leads to "conceptions that are so vague that they are unhelpful in shaping law and policy" (Solove, 2008, p. 40). If the concept of privacy is too specific, the same problem occurs when trying to shape regulations to alleviate privacy disruptions. Rather than crafting the perfect definition of privacy, Solove contends the focus should be on the specific types of problems and disruptions that occur (2002, 2008). One should understand privacy as a "set of protections against a plurality of distinct but related problems" (Solove, 2008, p. 171). Doing so will allow for flexibility of the concept to be useful during changes in social expectations of privacy while remaining stable over time (Solove, 2008).

Information Collection. This bottom-up approach to understanding privacy describes four general types of activities which may lead to privacy problems. The first are problems that can occur when information is collected about individuals (Solove, 2006, 2008). Surveillance and interrogation are collection activities that are common sources of privacy problems. Surveillance is problematic as it often negatively affects a person's behavior as they are watched. Interrogation is the act of pressuring individuals to provide information. The information benefits those receiving it, but problems arise when coercion is used to provide the information.

Information Processing. Solove's second area of privacy problems is information processing -what happens to the information once it is collected. These potentially problematic processing activities include aggregation, identification, insecurity, secondary use, and exclusion. Aggregation conflicts occur when entities compile isolated pieces of data to reveal facts about a person that would not have been known when the original information was collected. Identification can be problematic when data segments are used to connect to an individual. Insecurity is when stored data is inappropriately accessed by those who do not have permission to see the data. This insecurity can be intentional, as with identity theft, or accidental, as in the case of a health clinic mistakenly giving information about a patient's health records to the wrong person. Secondary use is when data is used for a reason other than for which it was initially collected, often without the subject's permission. Finally, exclusion is the harmful practice of not giving individuals access to their information. These individuals may not precisely know what data is collected about them or have the ability to change the use of the information.

Information Dissemination. Information dissemination is the third area of Solove's privacy problems, which refers to how collected information is revealed or spread to others. These dissemination problems occur in:

- breach of confidentiality
- disclosure
- exposure
- increased accessibility
- blackmail
- appropriation

- distortion (Solove, 2008, p. 136)

Breach of confidentiality is described as when a promise or expectation of secrecy about information is betrayed by the person or entity holding the information. Disclosure is similar to breach of confidentiality but differs in that there is harm to the reputation of the person whose information was made known. With a breach of confidentiality, the focus is on the "violation of trust in the relationship" (Solove, 2008, p. 142). Exposure is a privacy problem when sensitive information about a person's physical or mental condition is made known to others. When access to information already available to the public is amplified through a resource like the internet, this can lead to increased accessibility problems. This increased accessibility can be problematic when recipients easily exploit the information for purposes other than the reason it was initially collected. Blackmail is problematic when information control threatens the data subject. Appropriation occurs when one's identity is used to meet the goals of another and against how the individual wants their identity to be used or portrayed. Finally, distortion is a privacy problem when information about a person is changed or manipulated to change how that individual is perceived or judged by others (Solove, 2008).

Invasion. Solove's (2008) last category of possible privacy harm is invasion and includes the actions of intrusion and decisional interference. Intrusion involves actions that interfere with a victim's typical life activities and can lead to physical and emotional problems. More than just a physical intrusion, these activities also include inappropriate access to information about a victim. Decisional interference is when the government interferes with "people's decisions regarding certain matters of their lives," like contraception, sexual behavior, and child-rearing (Solove, 2008, p. 94). For example, laws regulating sexual or romantic relationships would fall under the category of privacy problems due to decisional interference.

Ohm's Framework on Use of Big Data

Ohm's (2014) work is not a theoretical framework, but it is a practical means to understand the common misuses of data and how to remedy those problems. This work consists of five changes for using information in the era of big data. These suggested changes are in the following areas:

- working with sensitive information
- the distinction of personally identifiable information
- gaps in legislation
- reminding researchers about humanity
- developing norms for responsible data science (Ohm, 2014, p. 104)

Ohm suggested the imposition or incentivization of these changes to protect the needs of individuals when scientists have greater access to large data sets.

Sensitive Information. Not all data has the same potential for harm, so Ohm's suggestions for privacy reform suggested regulations should focus on contexts that involve sensitive information (Ohm, 2014, 2015). These sensitive categories included health, financial, and educational information. These categories have some regulations in place right now, but there are other areas with little or no regulation because of their recent creation due to technological advances. Geolocation data, health information from fitness trackers, and databases of genetic information from services like 23andMe all deserve the categorization as sensitive information and the appropriate protections from laws and regulations.

Personally Identifiable Information Distinction. Anonymization of data is an effective means to de-link data from the individual who provided it. In some cases, privacy laws do not apply to data use for information not classified as personally identifiable information (PII).

Technology advances, especially in aggregation and analysis, have made it easy to relink anonymous non-PII data back to individuals. Ohm's framework (2014) for data use in the big data era recommended that privacy laws apply to all information, even if it is initially de-identified and not classified as personally identifiable.

Legislating Gaps. Ohm (2014) contended that some types of information should be declared off-limits for any collection, storage, or analysis. This work would be done intentionally through laws, so there are no gray areas in which this data is processed. An example is the federal Wiretap Act which makes it a felony to collect information transmitted over telephone or computer networks, with a few exceptions.

Reminding Researchers About Humanity. Ohm (2014) urged data scientists not to forget the people whose data they are analyzing. Studying big data sets typically does not require the researchers to interact with the subjects, and there is a fear that decisions that aren't beneficial for the unknowingly studied people could be made. Ohm suggested providing training to remind researchers of the lives of the people who provide the information they analyze.

Developing Ethical Norms. The community of researchers should develop and adopt ethical standards for responsible big data practices. These standards would be an essential step to eliminate ethical vacuums so the research community would not come under criticism from outside groups like lawmakers if a questionable study occurred. One way to do this is to have special standards for big data research in the human subjects review process. Ohm (2014) recommended this norm development come from within the field of big data research as those scientists are the ones who know the work the best and would be able to craft the most reasonable and practical ethical standards.

Nissenbaum's Framework of Contextual Integrity

Like Solove's work, Nissenbaum's approach (Barth et al., 2006; 2004, 2010) is based on real privacy problems rather than an attempt to develop a comprehensive conceptualization of privacy. Nissenbaum used the term *contextual integrity* to describe the concept because it focuses on the social structures or contexts in which information flows from one agent to another. This concept posited people don't simply act as independent individuals; they are part of interdependent social systems. Those systems' expectations and norms determine how information should flow among information users.

Key aspects of contextual integrity are *contexts*, *actors*, *attributes*, and *transmission principles (*Nissenbaum*,* 2010*)*. Contexts are the environments or situations in which people and organizations share information. There are norms within contexts that influence how information flows or is restricted. Contextual norms can be as formal as laws and regulations or the expectations of social relationships. The actors are the people in the context who provide, share, and use information. Attributes are the different types or descriptions of information transmitted within the context. The transmission principles are the conditions under which information transfers can or cannot occur. All these aspects of the context work together to determine integrity in the flow of information.

When the involved actors follow the contextual integrity norms, the flow of information has integrity. An example is when teachers follow expectations (transmission principles) for sharing student information. There is a disruption of integrity when the informational norms are not honored. This disruption could happen if a teacher gave sensitive student information to another member of the school context who, according to the contextual norms, should not have access to that information. Technology can enable threats to this integrity because of the ease of

transmission of information, intentional or accidental, that might not be in line with the norms of the context (Nissenbaum, 2010).

Contexts. There are four key constructs to help understand the concept of context (Nissenbaum, 2010). The first is that there are roles people play when it comes to privacy and the use of data. The *role* is a capacity in which people act in the context. This role is like the position of an administrator in a school district. The second aspect consists of people's activities while in their contextual role. In a school, the administrator would have many duties prescribed to their role, like developing schedules, interacting with students, and communicating with parents about their children. The third contextual feature is the norms that guide the behavior of those within these privacy contexts. These norms show what acceptable actions and practices (positive norms) are and what they are not (negative norms). The norms can be formal, like board policies and the school handbook, or based on social expectations, like not sharing sensitive information told to you by a friend. Finally, values are the last construct that underlies the contexts. Values can consist of the goals of the context and help center those people on a common purpose. All these factors influence the interactions, transactions, and communication within a context.

Norms. Norms are a central feature of contextual integrity, and Nissenbaum (2010) stated that they "define the duties, obligations, prerogatives, and privileges associated with particular roles, as well as acceptable and unacceptable behavior" (p. 133). Norms are the rules people ought to follow in a context. In addition to abiding by the norms, because the environment expects it, members also follow the norms because they are something they believe they should follow. An example of this norm influence is how educators share information with others in the school context about a student's documented disability. Based on state and federal

regulations, district policies specify what information can and cannot be shared about a student and to whom it is permissible to share that information. But even without these deliberate expectations, many educators would not share information about a disability because they know the potential harm to the student if they shared the information with the wrong person. The teachers follow those norms because they are aware of them and believe in the protections and expectations the norms provide. Privacy problems occur when information is shared or used in a way counter to the context's prevailing norms.

Actors. The people within a context are known as actors, the information subjects, and the senders and receivers of information. When considering the informational norms, it is important to know the contextual roles of all the actors in each situation. In a school example, teachers would be the senders and receivers of information about a student, the subject. Contextual norms regulate the teachers' actions as they discuss achievement data about a student they share. This type of information flow is appropriate in this context, but there would be an integrity issue if a teacher were to share that same achievement information with the parent of another student. It is the same sender, subject (the student), and student information, but the contextual norms would not support this information being received by this parent. School leaders can also be the senders and recipients of information, but they are also influential with all the other concepts of the CI framework. Knowing the actors and their contextual roles are key to understanding the integrity of the information flow (Nissenbaum, 2010).

Attributes. Attributes refer to the type of shared information in a particular context. The contextual norms vary according to the nature of the shared information. In the school setting example, there are different expectations for sharing information about a student's hot lunch choice compared to a medication they would take at school. Data about lunch choice is handled

much differently than information about a child's medical prescription. The difference in information attributes leads to different contextual norms for who can access the information and how it is transmitted (Nissenbaum, 2010).

Transmission Principles. This aspect of contextual integrity refers to the conditions under which information is shared. Transmission principles might include *confidentiality*, a prohibition about who can access information. Compulsion is another principle that would stipulate a subject provides information. These principles can impede or enhance the flow of information, but they depend on the context, what type of information is being shared (attributes), who the subjects are, and who is sending and receiving the information. Regarding a student's meal choice, very few conditions are necessary to regulate sharing this information. Because the type of information is not sensitive, there are few restrictions about who can know this information and the way it is shared. Contextual norms would not restrict the hot lunch choice being transmitted over the intercom from the teacher to the school secretary, with other students hearing the information. This would not be the case with sharing information about a child's medication intake. Transmission principles, like confidentiality, would restrict which actors could know this information. Because of the sensitive nature of medical information, there would also be restrictions on the method of communication used (Nissenbaum, 2010).

The contextual integrity framework can be used as a decision-making tool for avoiding privacy problems and as a predictor of where privacy issues might occur given a set of circumstances (Nissenbaum, 2010). When using the framework for these purposes, it is necessary to assess the critical aspects of the framework: *context*, *actors*, *attributes*, and *transmission principles*. Researchers or decision-makers need to know the context to understand what norms guide the scenario. Some contexts or settings, like schools or hospitals, may already

have a set of known norms, rules, and laws to guide information sharing. Other contexts may be ambiguous, and there are no apparent norms about how data can be transmitted. In those vague contextual situations, it is imperative to have a greater understanding of the other aspects of the framework.

Relevant Research Utilizing Contextual Integrity. The CI framework has been used to examine several information privacy topics involving education, children, and technology policies. It was the basis for understanding how parents' privacy expectations aligned with the Children's Online Privacy Protection Act (COPPA) regulations in the context of smart toys used by their children (Apthorpe et al., 2019). Birnhack and Perry-Hazan (2020) used Contextual Integrity to examine the conflict between the privacy expectations of high school students and the security needs of their school, which used closed-circuit television systems. Additional research used CI to explain the importance of less formal information flow norms when children decide whether to share technology passwords (Kumar et al., 2020). Mordecai's dissertation (2022) used Contextual Integrity to explore the attempts to balance the use of innovative technologies with the safekeeping of student data in a K-12 school district. Much of this research focused on district-level administrators' data privacy perceptions and practices. The findings highlighted the tension between protecting student information and ensuring the appropriate flow of student data for educational purposes.

Several studies have used Contextual Integrity to examine privacy concerns with student data in higher education settings. Ham's dissertation (2021) used aspects of CI to understand the use of university student data and the contextual conflict between what is legally permissible and what is ethical. Abbott's work (2020) also looked at conflicting contexts and how university data stewards made decisions on sharing student information. Ifenthaler and Schumacher (2016)

focused on university students' perceptions of how their education data was used by learning analytics programs. Students appreciated the ability of learning analytics systems to provide meaningful and effective educational experiences but were hesitant to share all types of information the programs needed to provide those experiences. Kim (2014) used the CI framework to explore the activities of the Federal Trade Commission and how the agency creates contextual norms in response to questionable use of consumer data, including the data of university students.

Nissenbaum's framework has also been used to explore policy implications in environments where technology is advancing beyond current regulations (Li, 2021; Shaffer, 2021; Winter, 2012). Shaffer's (2021) research included the examination of the perspectives of high school students regarding their privacy expectations while living in cities implementing smart technologies. Winter (2012) advocated for stronger public privacy policies in place of the self-regulation of the technology industry. Li's (2021) research focused on the increase in technology use during the COVID-19 pandemic and the emerging privacy concerns. While the study primarily centered on COVID-related health information, the author expressed concerns with the current federal regulations FERPA and COPPA and how they fall short of protecting student education data as schools rely more on online learning services and tools.

School Leaders in the CI Framework. The work of school leaders in the flow of information can be examined in multiple aspects of the framework. School leaders can participate as all or any of the actors within the core information flow process. They can send, receive, and even be the subject producing the information. For this general overview of leader presence within Contextual Integrity, school leaders are defined as building administrators, central office administrators, superintendents, and school board members.

Beyond the information flow process, what is additionally relevant for this study is the influence leaders can have on all other aspects of information flow. School policies and procedures are considered norms within the CI framework. These norms influence or restrict how information flows, what information flows, and who the information can come from and go to. School leaders are involved in almost all aspects of the life cycle of board policies. Board members, superintendents, and central office administrators are often the leaders most involved with the creation and adoption of district policies that regulate how student information flows within and out of the district. Other administrators, often at the building level, use policies to create procedures for students and staff members, which specify the step-by-step expectations and practices that support adherence to the policy. These procedural documents are also norms for the context of the school district as they set expectations for how information flows within the context of the district. School leaders can also set norms via policy and procedure for consequences of school community members when they do not follow the expectations of information flow.

Privacy Law in the United States

Just as it is complicated to define the concept of privacy, privacy laws in the U.S. are also considered confusing and piecemeal. Solove and Schwartz (2019) stated, "Data privacy law in the United States is currently a bewildering assortment of many types of federal and state law that differ significantly from each other" (p. 1). Whereas in the European Union, there is a comprehensive privacy law, the laws regarding privacy in the U.S. are described as "fragmented, inconsistent, and gap-ridden" (Solove & Schwartz, 2019, p. 1). Privacy information is primarily regulated by sector and industry. Different federal and state laws exist for the public and private sectors (Schwartz, 2013). This segmentation can lead to confusion and gaps in regulation,

depending on what type of institution or business is the creator or keeper of the information (Schwartz, 2013). While the following section is not a comprehensive review of all privacy law in the United States, it is positioned here to provide background about the current laws affecting this study.

The Constitution and Privacy

The United States Constitution does not explicitly use the word *privacy*, but the charter does address privacy in several areas of the Bill of Rights (Schwartz, 2013; Solove, 2016). The First Amendment supports privacy as it protects the freedom of association. This amendment also limits sharing on privacy grounds. In *Sorrell v. IMS Health Inc*., (2011) the Supreme Court found that a Vermont law banning identifiable data sharing for marketing purposes was unconstitutional as it over-regulated commercial speech (Hans, 2021).

The Third Amendment protects citizens' privacy as it prevents the government from requiring that soldiers stay in the homes of private citizens. In *Griswold v. Connecticut* (1965), the Supreme Court ruled unconstitutional a Connecticut statute that called for fines and imprisonment for the use of medicinal drugs which prevented pregnancy (Roraback, 1989). This law also applied to married couples. The court said that a right to privacy was inferred in the First, Third, Fourth, Fifth, and Ninth Amendments. Regarding the Third Amendment, the high court likened the invasion of the Connecticut law into the intimate lives of a married couple to the quartering of soldiers.

The Fourth Amendment applied to *Griswold* as people have a right to be secure in their homes. The amendment most applies to privacy as it limits the government's power for search and seizure (Solove, 2016). This amendment states:

> The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by an oath or affirmation, and particularly describing the place to be searched, and the persons or things doing the searching (U.S. Const. Amend. IV).

The Fourth Amendment has been examined in school settings on several occasions. In *New Jersey v. TLO* (1985), a school administrator demanded to look in the purse of a student accused of smoking cigarettes (Gahungu, 2018). Upon this search, the school official found marijuana, a significant amount of money, and a list of contacts thought to be related to the sale of the drugs. The teen was charged and convicted. The appellate court found in favor of the ruling, but the New Jersey Supreme Court overruled and said the search of the purse was unreasonable. In *Vernonia v. Acton* (1995), the U.S. Supreme Court held that the drug testing policy of the Vernonia School District in Oregon was a reasonable search of student-athletes (Rammell, 2020).

In *NN v. Tunkhannock Area School District* (2011), a Pennsylvania student said school officials violated her privacy when her cell phone was seized and searched. School staff found nude photos of her on the phone and suspended her from school for three days (Black Jr & Shaver, 2019). The student was also threatened with child pornography charges if she did not comply with completing a re-education course on sexual violence and victimization. A Pennsylvania U.S. District Court denied the defendant's motion for judgment and said the student's case against the school district and District Attorney could proceed. The student's attorney from the ACLU said, "Schools have no more right to look through personal photographs stored on a student's cell phone than they have the right to rummage through her purse, read her

diary and mail, or view her family photo album" (Ito, 2010, p. 8). The school district settled out of court for $33,000 (Ito, 2010).

The Fifth Amendment states that the government cannot compel individuals to provide incriminating information about themselves. *New Jersey v. T.L.O.* (1985) references this amendment as a school administrator forced a student to allow a search of her purse. With *In re Tateana R.* (2009) and *State v. Schloegel* (2009), courts found that school officials and resource officers do not need to give Miranda warnings to students when questioned (Russo, 2013). However, *In re R.H.* (2002) found that students' rights are violated when questioned by law enforcement officials and not given the Miranda warning (Russo, 2013).

The Right to Be Let Alone

While not a law, the work of Warren and Brandeis in "The Right to Privacy" is considered one of the most influential American definitions of privacy and serves as the basis for many subsequent privacy laws (Bratman, 2002; Solove, 2016; Warren & Brandeis, 1890). The growing prevalence of newspapers in the second half of the 19th century prompted their article. Newspaper circulation increased by 1000% from 1850 to 1890, and the papers increased the reporting on more sensational topics like scandals, hearsay, and people's private lives (Bratman, 2002; Solove, 2016). Warren and Brandeis (1890) commented, "The press is overstepping in every direction the obvious bounds of propriety and decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry" (p. 196). They were also concerned with technological advances in photography. The Eastman Kodak Company produced a hand-held camera for general public use, which made it easy for people to take candid photos in public spaces. The authors were concerned about the future use of these cameras by the sensationalistic press that would "invade the sacred precincts of private and

domestic life, and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops" (Warren & Brandeis, 1890, p. 195).

At the time of the article's publication, the laws did not provide much legal protection for an individual's privacy. Defamation laws were a deterrent to libel, slander, and false information but did not apply to sharing true and private information (Bratman, 2002; Solove, 2016). Contract law guarded privacy in legal relationships between the involved parties but did little to thwart invasions of privacy by third parties to the contracts. Existing property laws of the time did little to protect the individual's rights. These laws would protect the production of publications but not prevent publication in the first place (Bratman, 2002; Solove, 2016). Brandeis and Warren (1890) argued that common laws should protect an individual's "right to be let alone," the ability to determine when to share their thoughts, feelings, and emotions with others. They suggested these rights would be defined and protected through tort actions for damages due to these violations of an individual's privacy. They also offered "substantial compensation" for the victims of libel and slander (Warren & Brandeis, 1890).

Soon after, states began to pass laws protecting individuals' privacy. In 1903 the state of New York enacted a statute protecting privacy after a flour company used the lithograph of a woman on their packaging without her permission (Webner, 1994). A similar case occurred in 1905 when an insurance company used the plaintiff's image without permission. The Georgia Supreme Court recognized the tort as an invasion of privacy *(Pavesich v. New England Life Insurance Co.*, 1905).

Prosser (1960) examined 300 privacy cases after the Warren and Brandeis publication and found four types of torts in the case law. The first was *intrusion upon seclusion,* where

others invaded another's private affairs through electronic eavesdropping, clandestine photography, and surveillance. The next area of infringement was the *public disclosure of private facts*, where details of a person's life were shared when it was not a legitimate concern of the public. The next area of privacy disruption was when a person was brought to public attention in a *false light*. The final area that Prosser identified was *appropriation,* when a person's name or likeness was used without their permission. Most states now recognize these torts in their courts (Richards & Solove, 2010; Solove, 2016).

Privacy Laws at the End of the 20th Century

The end of the twentieth century saw the expansion of the internet, an increase in the use of email, and new challenges to privacy protection (Solove, 2016). The private sector used the increased computing power, especially for marketing. Businesses and corporations collected large amounts of consumer information like purchase history, demographic data, product opinions, and psychological profiles. With the advent of computerized databases, advanced search tools, and communication methods, businesses could use that information to target individual consumers with products matched to their profile.

Lawmakers enacted several new laws in the 1990s in response to new technologies and new uses. The Telephone Consumer Protection Act of 1991 allowed people to ask that telemarketers no longer call them. The Drivers' Privacy Protection Act of 1994 required that the state motor vehicle departments get permission from owners before selling their vehicle records information to marketers (Solove, 2016).

One of the most significant pieces of privacy legislation was the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and it is the first piece of federal law to specifically address health privacy (Solove, 2016; U.S. Department of Health and Human

Services [HHS], 2020a). The Department of Health and Human Services (HHS) drafted the regulations of the law, and they include the "Privacy Rule" and the "Security Rule." The Privacy Rule establishes national standards to protect a person's medical records and applies to health insurance companies and healthcare personnel (HHS, 2020a). This rule also gives patients the right to receive and examine copies of their health records and make corrections if needed. The Security Rule outlines standards for procedures to ensure the "confidentiality, integrity, and security of electronic protected health information" (HHS, 2020b, para. 1).

Education Privacy Laws

Education has a history of privacy legislation and is impacted by many of the abovementioned regulations. As with national privacy legislation, no all-inclusive bill covers privacy issues in education for the students in the system. The three acts that are most directly applicable to student information are the Family and Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children's Online Privacy Protection Rule (COPPA).

Family and Educational Rights and Privacy Act

FERPA was enacted in 1974 and is a federal law that aims to protect the privacy of the educational records of students in public and private schools or Local Education Agency (LEA) that receive funding from the United States Department of Education (U.S. Department of Education [USDOE], 2022). Examples of educational records include student background information, grades, standardized test results, psychological evaluation information, disability reports, and anecdotal information from educators about the academic performance and behavior of the student (USDOE, 2022). FERPA does not regulate student-produced content (essays, digitally produced information, artwork, etc.) unless it includes Personally Identifiable

Information (PII). Information is classified as personally identifiable when an examination of the data can identify an individual student. Any educational organization that violates the FERPA regulations can be denied federal funds.

Many exceptions allow student records to be released to other parties without parental consent. For example, school officials may release records for educational purposes they deem appropriate. An example of this is when an organization conducts a study on the school's behalf (USDOE, 2022). *School officials* can include "contractors, consultants, volunteers, and other parties to whom an educational agency or institution has outsourced institutional services or functions it would otherwise use employees to perform" (Molnar & Boninger, 2015, p. 10). Schools can release information to these designees without parental permission.

Under FERPA, parents have the right to obtain a copy of their school's policies concerning access to educational records and the ability to review those records and request any needed corrections. Parents also have the right to stop the release of any PII and choose to opt out of having their children's directory information released. Directory information typically includes the name and address of a student (USDOE, 2022).

The USDOE (2022) provided guidance and best practices for schools when they purchase or agree to use online educational programs. The department recommends that schools examine each service case-by-case to ensure its use complies with FERPA regulations. They also suggest that educational organizations maintain written contracts with online services and that the contracts address what data is collected, with whom that data is shared, and how the data is stored and secured. The contracts should also address how the students and parents can access the student data, how the data is destroyed upon the end of the contracted service, and define

indemnification should a vendor not comply with relevant laws and regulations. It is important to note that these guidelines are not requirements of the statute.

Analysis has found that FERPA has been weakened through regulatory changes, making it easier for schools to collect and share information with private education corporations (Strickland, 2019; Weber, 2016). In 2008 and 2011, the USDOE changed the law's "authorized representative" definition, allowing school districts to share records with outside contractors without parental consent (Weber, 2016). Another concern with FERPA is that the law states that only those with a legitimate educational interest in the student information should have access to it, but that legitimate interest test has been vague and hard to define (Abilock & Abilock, 2016; Babler et al., 2017). Another area of contention is determining what constitutes an *educational record,* the protected information under FERPA. Service providers and vendors often use non-records information for marketing purposes or sell it to other companies (Sabourin et al., 2015). School organizations are sometimes the source of concerns as they improperly use FERPA to avoid disclosing information during a legal open records request (Sabourin et al., 2015). While there are liabilities a district would face for FERPA violations, these federal punitive actions do not apply to the private vendors themselves (Abilock & Abilock, 2016).

Protection of Pupil Rights Amendment

Not as far-reaching as FERPA, the Protection of Pupil Rights Amendment was enacted in 1974 and amended in 1978 and 1994 to protect students' sensitive personal information collected in surveys, evaluations, and analyses (Daggett, 2008; Sallay & Vance, 2020). The law requires that schools obtain written consent from parents for their minor children to participate in any USDOE-funded survey or project that may collect information from several sensitive areas.

Those areas include political affiliation, income, psychological issues, sexual behavior, illegal or anti-social acts, and religious practices (USDOE, 2020a).

PPRA was updated as part of the No Child Left Behind Act of 2001 and requires schools to work with parents to develop policies that address several pertinent areas regarding collecting student information in surveys (Daggett, 2008; USDOE, 2020a). These policies should address how parents can review surveys before students participate. The policies should also provide guidance when information collected from students is shared for marketing purposes (USDOE, 2020a).

One concern with PPRA is that it only applies to surveys and research funded through the U.S. Department of Education. Other parties not supported by the USDOE seek similar sensitive information, and PPRA does not apply to those activities. In addition, PPRA requires local education agencies to notify parents of their rights, but often those notices are part of blanket notices given to parents at the beginning of the school year. These notices often do not specify when these surveys will occur, how parents can access them for review, or how they can opt their children out of these activities. Another concern with the law is that districts do not need parental consent to use students' personal information to develop, evaluate, or provide educational products or services (Weber, 2016; USDOE, 2020a). Third-party private technology companies often provide these evaluation services.

Children's Online Privacy Protection Act

Where FERPA and PPRA regulate the use of information about students in educational agencies, the Children's Online Privacy Protection Act (COPPA) was enacted in 1998 to govern the collection of information from children in environments largely away from school. COPPA defines children as individuals under the age of 13. According to this regulation, websites that

market their services to users under 13 must post privacy policies and obtain parental permission to collect, use, or disseminate personal information from children. Parents also have the right to review the terms of service and privacy policies of their children's accounts with these services.

COPPA only applies to sites intended for children ages 13-17 and only if the site's operator has verifiable knowledge that it is collecting personal information from a person under 13. Many websites, especially social media, specifically state that their service is for people aged 13 and older. Still, it is easy for users under 13 to falsify their birthdates when signing up for these online accounts. COPPA does not apply to teens, who are often the majority of users of digital technology. Another concern with COPPA is the broad interpretation of what it means to be a school official and have legitimate access to student data. Education technology companies have used the school official exception rule to take advantage of local school officials unfamiliar with the complexities of the law or push the compliance responsibility to school staff (Electronic Privacy Information Center, 2019; Herold, 2017; Skowronski, 2022). The school can legally consent on behalf of all its students for using PII, but parents would have to take individual action to stop sharing this information (Abilock & Abilock, 2016).

In response to the increased use of educational technology during and after the COVID-19 pandemic, the Federal Trade Commission (FTC) released a policy statement in May 2022 to address new concerns with children's information privacy while using educational tools (Federal Trade Commission, 2022). While the language of COPPA has not changed, the FTC statement shares that there will be more focus on enforcing the regulation in several key areas. Companies can not require disclosing more personal information than is reasonably necessary for using the technology resource. The policy statement also clarifies that education technology companies are limited in using the information they collect from students. The student data can be used for the

purpose of the educational resource, but it can not be used for commercial purposes not related to the school's contracted online service. Another area of enforcement focus is the retention of student information. Companies can not hold data longer than necessary to use the educational resource. The FTC will now ensure that educational technology companies have procedures to ensure the confidentiality and security of students' personal information. Regarding earlier criticisms of education companies relying on administrators, staff, and parents to monitor and enforce COPPA compliance, the Federal Trade Commission makes a firm statement:

> In case an ed tech company is thinking about passing compliance off to school administrators, parents, or others – for example, through contract provisions or terms of service – the Policy Statement makes it clear that's a hard no. The responsibility to implement strong privacy protections rests squarely on ed tech companies and it's an obligation they can't shirk (Fair, 2022, para. 11).

Educational Technology and Data Privacy

To understand present-day concerns with data privacy within educational technology systems, this section of the literature review will begin with a historical review of educational technology growth in schools and outline the early concerns regarding the privacy of student data within these connected systems. As in other areas of society and industry, technological innovations are also undoubtedly present in education. Educational agencies have always collected, stored, and analyzed data, but these methods changed significantly when lawmakers enacted No Child Left Behind (NCLB) in 2001. The law increased the accountability requirements, and the federal government required states and districts to develop longitudinal data systems to collect information to analyze student achievement and program effectiveness (Krueger & Moore, 2015; Trainor, 2015). State and federal organizations, along with private

companies, developed computerized databases to track whether schools were progressing toward improving their students' achievement.

At the same time as the new data system requirements, there was increased usage of digital devices and online education tools and programs. Districts were taking advantage of digital tools like mobile computers, software as a service, learning management systems, automated response collection, and online learning programs (Krueger & Moore, 2015). These resources require student information to provide rich and adaptive experiences for the student user (Krueger & Moore, 2015). Like the new databases, these programs were the creation and property of third-party vendors not under the education agency's control. These new tools led to an exponential increase in available data. In addition, these tools resulted in abundant mouse clicks, keystrokes, swipes on mobile devices, and information from motion sensors and facial recognition tools (Wang, 2016).

Growth of Learning Analytics

In response to the massive amounts of new data, the field of learning analytics (LA) grew within education to collect, analyze, and report on all this information with the intent of improving student instruction and assessing the effectiveness of curriculum, educational programs, policies, individual educators, and schools (Reidenberg & Schaub, 2018; Rodríguez-Triana et al., 2016; Sabourin et al., 2015; Wang, 2016; Weber, 2016). The analytics field was informative of traditional classroom-based instructional methods, but it also provided valuable information for digital tools like learning management systems, responsive tutoring programs, and collaborative platforms (Wang, 2016). The field of learning analytics and the associated technological tools allowed researchers and education leaders to “tap into student learning activities and social interactions at a scale that [had] never been seen before in education”

(Wang, 2016, p. 381). Beyond just the analysis of achievement scores, educational analytics could also derive meaningful information from how and when the students interacted with the digital learning platforms, what resources they read and what order they read them, and the students' participation in online discussion forums (Reidenberg & Schaub, 2018). With big data and learning analytics, educators could tailor instruction to individual needs, and instructors could closely monitor student progress and quickly respond with appropriate educational activities (Reidenberg & Schaub, 2018; Wang, 2016).

Concerns with Big Data and Learning Analytics

With learning analytics, these systems need large amounts of student data. This information collection leads to inherent risks to the students' privacy who produced the data (Reidenberg & Schaub, 2018). Reidenberg and Schaub (2018) used aspects of Solove's (2006) taxonomy on privacy to categorize harms with big data and student privacy. The most prevalent harm was the large-scale collection and dissemination of student information, leading to secondary users' inappropriate use of the data. Another harm is the fear of surveillance as students' online behavior is tracked as they work through the various learning platforms. The lack of transparency is another possible harm as it is not always clear what data is collected and how it is used. Schools don't always notify parents about using their children's data in cloud services. Often, these collection and use methods are so complex that it is difficult for school officials to explain them to parents (Reidenberg et al., 2013). Because "big data programs rely on data sharing rather than confidentiality," the information of students is not always kept securely (Reidenberg & Schaub, 2018, p. 7). As a result, multiple vendors and organizations have access to sensitive information. Another harm is that students and parents rarely have control over using the student's personal information in big data analytic environments. If

students didn't want to have these vendors using and sharing their data, they could opt out and not use the learning tools; however, not participating would skew the data that already exists in the platform or collected from another source of information.

While learning analytics continues to grow as storage and analytic methods advance, research has suggested several guidelines on how the field can provide quality service and information to schools while maintaining an appropriate level of privacy. Rodriguez-Triana et al. (2016) provided guidance for the ethical issues in the burgeoning field of learning analytics, encouraging more attention to issues such as consent of students and families, transparency of data collection, defining access to the information, and maintaining the privacy of the data and the students who provided it. Recent research proposes a collaborative design process in schools using Learning Analytics services. The strategy emphasizes transparency and trust-building with educators using analytics tools and services so there is continual communication among the school site educators, researchers, and learning analytics developers (Ahn et al., 2021; Rodríguez-Triana et al., 2021; van Leeuwen et al., 2021).

Shift from Localized Storage and Analysis

Most districts did not have the resources to develop or maintain their own data systems that were needed to satisfy the new regulations and increased amount of educational data, so they looked to private off-site vendors, or cloud services, for this kind of service (Molnar & Boninger, 2015; Reidenberg et al., 2013). Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider instruction" (Mell & Grance, 2010, p. 3). Cloud service companies offered an advantage to local

schools as they could update storage software, maintain security issues, and fix common software bugs without effort or knowledge from the district clients (Weber, 2016).

Concerns with Cloud Vendors

Cloud computing was a developing technology as the National Education Technology Plan was enacted in 2010, and storing student information in this manner led to concerns about contracts with vendors, ownership of the data, security of the storage systems, and control of who could access the student information (Bathon, 2013a). Data stored on the internet is easily shared, and this was a challenge for school IT personnel accustomed to closed systems where information stayed within their district network. Establishing and understanding contracts with storage and data analysis vendors was another new challenge for school districts. Bathon (2013c) pointed out the necessity for those contracts to specify that the district owns the data and is the authority on how and with whom the student information could be shared. Along with the concern for the safe keeping of this student data was the concern of costly legal liability for the district should a data breach occur (Bathon, 2013b).

Reidenberg et al. (2013) closely examined the practices of U.S. school districts as they contracted with cloud computing companies and transferred student data to them. As early as 2013, they found 95% of districts used cloud services for storage, analysis, classroom activities, student performance tracking, and services for their transportation and nutrition departments. With so many school systems using cloud services, the authors learned that vendor contracts are "poorly understood, non-transparent, and weakly governed" (Reidenberg et al., 2013, p. 2). Few districts had policies in place for online services, and a majority had issues documenting their service contracts. Their study found that districts commonly gave up control of student data due to missing critical features in their vendor contracts. A primary concern with those inadequate

contracts is that they don't address the parents' rights to notice, consent, and access their children's data. Finally, the research found that cloud service agreements did not appropriately address data security and failed to specify retention timeframes for student information (Reidenberg et al., 2013).

Parental Support of Student Data Use

A 2016 study by the Future of Privacy Forum (FPF) examined parents' perspectives on how student data is collected, stored, analyzed, and shared within educational settings (Future of Privacy Forum, 2016). The survey in the study found very strong support from parents when collecting student data for grades (97%), attendance (94%), special needs support (92%), standardized test scores (92%), and disciplinary records (90%). The level of support was lower for the collection of race and ethnicity information (53%), parent marital status (45%), family income (37%), and social security numbers (35%). There was high support for principals (92%) and teachers (91%) having access to student records, but less comfort for educational device and software companies (43%) having student information. These results show parent comfort was higher for individuals who are connected to their children's education.

There was high parent support for using data to tailor instruction (90%), support struggling students (85%), and personalize learning (82%), but little support for companies to use the information to market services (35%) and create targeted ads (23%). More than 70 percent of parents support adequately protected electronic records for educational purposes, but 84 percent of parents are concerned that this information could be hacked, and 68 percent are worried about it being used against their children by colleges or employers. The report showed that parents understand the benefits of electronic records but have concerns about possible misuse or breaches of security with student information. These concerns were similar to general

population surveys regarding data security with other governmental groups, credit card companies, and retailers.

Another recent parent survey (Center for Democracy & Technology, 2020) examined general educational concerns, and student data security issues were present within those top identified concerns (Table 1). While not the top concern, data privacy and security were concerns for the parents in this study.

Table 1 - Parent Concerns from Center for Democracy & Technology Survey

Identified concern	
Quality of education	76%
School stress/pressure	72%
Bullying	71%
School violence	70%
Unauthorized access of online activities or unauthorized communication with them online	68%
Student enjoying school	66%
Making adequate academic progress	65%
Mental health	65%
Student data privacy (e.g. who is authorized to access school-related information about your child)	64%
Cyberbullying	64%
Not being able to monitor/limit what your child has access to/sees on the internet	64%
Student information security (e.g. protecting school information from breaches or unauthorized access)	61%

Note. Data privacy items from the survey are bolded in this table. The value in the right column represents the percentage of parents reporting either "very concerned" or "somewhat concerned."

Another item on this survey asked who parents thought were most responsible for student data privacy and security. School administrators were tied with parents at 52% (respondents could

pick up to 3 roles). When asked who parents would approach with questions or concerns about data privacy and security, building-level administrators were identified most frequently at 59%, teachers and aides at 46%, and the district superintendent at 43%.

The FPF parent survey also asked parents about their knowledge of the various federal laws and regulations that address student data use. Only 21 percent of the parents in the study knew there were federal laws and understood how public schools could use student information. Similarly, 21 percent of the parents were aware of how the laws regulated companies' use of student data. Less than half of the parents (40%) said they received information from their children's school regarding directory information. Still, only 28 percent remember receiving information about their rights to opt out of having their children's data included.

The Future of Privacy Form report included several recommendations for creating a trusted learning environment with parents when schools and companies providing educational services collect and use student information. For example, the report said schools should provide more training for administrators and teachers to use educational technologies and frequently inform parents about these new tools. The FPF report also recommended schools should create clear policies about using and disclosing student data and include parents as part of that process to keep them informed and address their concerns (FPF, 2016). These activities, providing professional development, policy implementation, and parent communication, have all been effective practices of district leaders (Dexter et al., 2017; Hitt & Tucker, 2016; Leithwood et al., 2010; Waters & Marzano, 2006).

Impact of the COVID-19 Pandemic

In the spring of 2020, the COVID-19 pandemic impacted the education experience of nearly 1.6 billion students (91.3%) in P-12 settings worldwide (United Nations Educational,

2022). In the United States, 77% of public schools reported moving some instruction to online methods in the spring of 2020 (Berger et al., 2022). The effect of the pandemic was still present at the beginning of the 2020-21 school year, as 62% of schools remained in virtual environments (Roche, 2020). Bushweller and Lloyd (2021) referred to this time as the "most disruptive period in the history of modern education" in their reporting of K-12 data regarding the pandemic (p. 2).

As most schools closed their familiar face-to-face instruction, they turned to educational technology tools and resources to continue their school programs. Anderson (2020) referred to this wide-scale and abrupt shift as "the world's biggest educational technology (edtech) experiment in history. With 1.5 billion students out of school and hundreds of millions attempting to learn online, the experiment will reshape schools, the idea of education, and what learning looks like in the 21st century," (para. 4). Educational technology companies were "positioned as a frontline emergency service," as they partnered with K-12 and higher education institutions to help these organizations continue providing instruction (Williamson et al., 2020). The use of online educational technologies peaked during the height of the pandemic, but it is expected that schools will continue to rely on these tools and vendor partners to provide virtual and blended learning services (Arnett, 2021; Bushweller & Lloyd, 2021; Data Quality Campaign, 2020b; Future of Privacy Forum, 2022; Grant et al., 2020).

The increased use of remote education technology services also focused on student privacy issues, with the initial concern being student health information. The immediate issue was how the COVID-19 pandemic required collecting and sharing student health information and that schools faced "new tensions around student privacy that will need clear guidance from federal and state policymakers" (Bailey & Hess, 2020, p. 7). The U.S. Department of Education and professional education organizations put forth guidance documents regarding current federal

regulations, and general privacy practices to address student health information records (Reddy & Vance, 2020; Student Privacy Compass, 2020b; U.S. Department of Education, 2020a).

In addition to student health information, the increased use of technology during the pandemic highlighted other privacy concerns for students. Many instructors and students using the video conferencing platform Zoom for live instruction were victims of "Zoom bombing" where people would disrupt these sessions with abusive language and images (Harris, 2020; Li, 2021). Using new geo-tagging applications for COVID-19 contact tracing and exam-proctoring programs brought forth novel concerns for student privacy (Bagchi et al., 2021; Kshetri, 2020; Li, 2021; Talukder et al., 2020). Students also experienced a sense of privacy loss due to the virtual instruction in their homes instead of school buildings (Li, 2021; Pandit et al., 2020). Students' homes were viewable to classmates and instructors when using video platforms, and some students were hesitant to share their ideas regarding educational subjects while family members were nearby. There was an increased number of reported cybersecurity incidents in schools in 2020 due to the increased reliance on technology devices and online resources (Levin, 2021). These incidents included data breaches from students and staff, denial of service attacks, ransomware, malware and phishing incidents, and social engineering scams. At least 75% of these reported data breaches in 2020 in K-12 schools were related to issues with district vendors and other resource partners (Levin, 2021).

In response to the new focus on student privacy issues and educational technology use during the pandemic, several recommendations have come forth from research and privacy and educational organizations. First, education decision-makers should understand federal and state data privacy regulations and examine their educational technology partners' privacy policies and practices. This knowledge will ensure consistent safeguarding of the information they use and

share (Bagchi et al., 2021; Bailey & Hess, 2020; Data Quality Campaign, 2020b; Levin, 2021; Student Privacy Compass, 2020b). Second, school leaders should train staff members, students, and parents on data privacy and how student information is used in school technology systems (Data Quality Campaign, 2020b; Ishmael et al., 2020; Student Privacy Compass, 2020b). Third, education leaders should examine their communication procedures to ensure transparency with stakeholders by sharing what student data is collected, how it is used and shared, and how the information is stored (Bagchi et al., 2021; Student Privacy Compass, 2020b).

There is also an emphasis on establishing strong and effective policies for overall student data use in schools. The Data Quality Campaign urges state education leaders to consider legislation, "Protecting student data privacy starts with strong policies and practices," (2020, p. 2). Establishing data governance policies is suggested as a means for state education agencies and local districts to ensure they effectively and appropriately use student information (Data Quality Campaign, 2020b; Student Privacy Compass, 2020b). The data governance approach encompasses the rules, policies, and procedures and identifies the individuals within education systems responsible for all aspects of student data. Data governance includes what data is collected, how and with whom it is shared, how it is used, how it is stored, how long it is kept, and how it is safely discarded when no longer needed (Student Privacy Compass, 2020b).

Additional Post-Pandemic Privacy Concerns

The COVID-19 pandemic led to an unprecedented surge in the use of technology for education, but remote work, communication, and entertainment were also beneficiaries of these digital tools. Along with the increased usage of these resources, privacy and data protection concerns have gained renewed attention. One notable example is the widespread popularity of TikTok, a social media platform that faces significant scrutiny due to its data collection practices

and its ties to a Chinese company(Shu, 2020; Trifiro, 2022). The application provides a platform for creative expression and social connection and is especially popular among younger users. However, the application has raised significant concerns about user privacy, as it collects vast amounts of user data that could be used for surveillance, profiling, or manipulation by the Chinese government, an economic and military rival of the United States (Williams & Center, 2020).

The growth of artificial intelligence (AI) during the post-pandemic era has further intensified privacy concerns. As AI systems become increasingly integrated into various aspects of our lives, the collection and analysis of personal data have reached unprecedented levels. In addition, many AI systems, such as facial recognition and predictive analytics, rely on large datasets to improve their accuracy and effectiveness (Almeida et al., 2022). However, the widespread use of these technologies raises questions about the ethical implications of mass data collection, the potential for misuse of information, and the attrition of personal privacy (Anshari et al., 2022; Aung et al., 2021). Moreover, biased algorithms and a lack of transparent human activities in AI decision-making processes can lead to unintended consequences, further intensifying the debate around the trade-off between technological advancements and individual privacy (Kostick-Quenet et al., 2022; Schwartz et al., 2022).

Similar to the attempt to preserve student data privacy in modern educational technology systems, governments, industry organizations, and individuals must work together to develop robust legal and ethical frameworks that balance innovation and privacy protection. This includes establishing clear guidelines for data collection, storage, and usage and developing technologies that enhance privacy without impeding the benefits offered by AI and social media platforms. Additionally, promoting transparency in AI decision-making and fostering a culture of

privacy awareness among users are crucial steps toward ensuring that the digital landscape develops in a manner that respects the fundamental right to privacy while harnessing the potential of technology to improve our lives.

Regulating New Technologies

Before the boom of the internet and the abundance of cloud-based education programs and services, most schools could easily comply with these privacy regulations and security procedures. These duties were often left in the domain of the IT professionals in the district (Anderson, 2019). Security measures became much more complicated as the internet, online services, and social network platforms grew and became more powerful. Compliance was also not as easily attainable to use these resources while keeping data and students safe. District personnel must also be familiar with data breach contingency plans and other legal issues (Bathon, 2013b). One initial approach to compliance and safety was the lock-down approach to the district network, severely restricting which devices, programs, and sites students could use. This approach was often paired with rigid acceptable use policies (AUPs) that spelled out a list of restricted activities and accompanying consequences for running afoul of the guidelines. These attempts to control safety and privacy made it difficult for educators and students to use the innovative digital resources that led to increased student engagement and achievement. As a result, districts shifted away from strict use policies to ones that highlight the positive and acceptable use of technology tools and resources (Krueger & Moore, 2015).

These shifts in privacy practices and expectations were not only new territory for the districts as many ed-tech startup companies were experiencing challenges in this growing field. A Carnegie Mellon University case study examined ed-tech startup companies' practices regarding student data privacy issues (Babler et al., 2017). This research found that these new

startup companies often did not prioritize student data privacy as they were more concerned with appealing to new customers and further developing their products. The second finding was that nascent companies did not have formal communication strategies to discuss data privacy as they had limited funds and staff members. When these companies had privacy policies in place, they took a standardized approach, used boilerplate statements from their industry, or adopted language from other ed-tech companies. Finally, the study found that even though they did not prioritize student data privacy, the innovation in their products and services continued to grow (Babler et al., 2017).

The Case of InBloom

The rise and fall of the non-profit education data analytics company InBloom was the first example of the significant concern about using student data. The initiative was founded in 2011 with $100 million from the Bill and Melinda Gates Foundation. The project aimed to create a centralized platform for data storage and sharing, curriculum, and learning applications (Bulger et al., 2017; Strickland, 2019). The idea was to create a service that would serve multiple states, as compared to past practices of isolated data use, and be an environment for sharing best practices with information analysis and instruction. Greg Mortimer, a Chief Information Officer for one of the early InBloom participant districts, shared, "The classic challenge everybody in K-12 talks about is we have data from all these disparate systems. How do we grab that data in a timely fashion and use it to inform instruction and hope we move the needle with student achievement?" (Bulger et al., 2017, p. 9).

Public Distrust of Big Data. At its launch in 2013, several other events led to public scrutiny of data collection and use. That summer, Edward Snowden disclosed how the U.S. National Security Agency accessed millions of Americans' phone records and internet

communications. Later in the year, Target had a data breach of credit card information for 70 million customers. These data security issues occurred when there was a push for national testing and a growing mistrust of large philanthropic organizations suspected of being key players in privatizing education (Bulger et al., 2017). The CEO of the Data Quality Campaign, Aimee Guidera, summarized the concern, "the issue is InBloom and education data collection became nuclear and it became synonymous with Big Brother, Edward Snowden, Target, making teachers into robots, putting teachers out of business, social engineering, lack of parent control" (Bulger et al., 2017, p. 14).

Concerns with InBloom. This also occurred when the Common Core and the Race to the Top programs were criticized in a movement of resistance to big government initiatives. In addition, the public saw extensive data collection and analysis programs like InBloom as a means of harsh school accountability and the concern that student data was vulnerable to breaches and used as a profit resource for third-party companies (Bulger et al., 2017). Parent and community groups coalesced with strong opposition at the local school district level with town halls and informal meetings where participants voiced their concerns with security, student data use, and opposition to the InBloom project.

The initial data collaborative in January 2013 consisted of districts in nine states with 11 million students working with InBloom. However, by November of that year, only three of these states were still working with InBloom after months of public scrutiny from parents, school officials, and lawmakers. Even New York City mayoral candidate Bill De Blasio weighed in against centralized data sharing, "As mayor, I will protect students' privacy and stop this needless invasion of privacy" (Bulger et al., 2017, p. 21). The end finally came when the New

York state budget included a clause to make it illegal for the state to share personally identifiable student information with a private cloud-based entity, effectively ending the InBloom initiative.

New Privacy Practices and Policies. The public controversy over the InBloom initiative, the general environment of concern for data security and privacy, and the continued growth of digital educational services led to an examination of practices, policies, and legislation around the country. Jat Pannu, Chief Operating Officer of IlliniCloud, stated:

> I think InBloom was a quantum leap forward. It not only galvanized the marketplace towards a common area of opportunity for student achievement, but it also put a spotlight on an area where we should have been focusing a long time ago… [It] created the activation energy for vendors to now work with different organizations to solve the student data privacy issue because now everyone realized what's the type of risk that's associated with the data that they're collecting and keeping and storing (Bulger et al., 2017, p. 24).

Educational technology vendors, education organizations, and other interested parties developed and introduced the Student Data Privacy Pledge in 2014 through the Future of Privacy Forum and The Software and Information Industry Association (Bulger et al., 2017). President Obama endorsed the initial pledge, consisting of 12 key commitments based on federal law and industry regulations for collecting, storing, maintaining, and using students' personal information (Future of Privacy Forum, 2020). The pledge was updated in 2020 to align it to current state and federal privacy regulations and expand the type of data covered (Future of Privacy Forum, 2020). The last press release from the Privacy Pledge consortium was in November 2020, with 439 educational technology companies noted as signatories.

Attempts to Update Federal Student and Children's Privacy Legislation

There was an effort to update FERPA in 2014 as Senators Markey and Hatch introduced the Protecting Student Privacy Act in July 2014 (Markey & Hatch, 2014). The bill's goals were to require schools to protect the PII of students, prohibit them from using or releasing that information for marketing, and give parents the right to access, correct, or delete any inaccurate data in the education records held by private companies. The bill also aimed to restrict the amount of PII schools could share with third parties, required disclosure of which outside parties have access to student data, and required these outside groups to have comprehensive security policies and procedures for storing and using student information. The senators wrote in The Hill in 2015:

> We need to update FERPA to put parents in control of their children's most personal information. We need to ensure private companies continue best practices and do not utilize students' information to advertise products. We need to empower schools to restrict the amount of time a private company can hold on to student records, provide parents with the right to access personal information about their children that is held by private companies, and back-up companies who institute comprehensive data security programs. In short, our proposal is guided by the principle that parents should control their children's most private information, regardless of whether that data sits in the school's file cabinet or a private company's computer (Markey & Hatch, 2015, para. 3).

The bill was introduced in 2014, 2015, and 2017, and referred to the Senate Committee on Health, Education, Labor, and Pensions but never made it out of the committee (Protecting Student Privacy Act, 2014, 2015, 2017).

The Children and Teens' Online Privacy Protection Act, or COPPA 2.0, was introduced in the Senate with bipartisan support in 2019 (S. 748, 2019). The bill would have codified recent areas of focus from the Federal Trade Commission by limiting educational technology companies from requiring the disclosure of more student data than is necessary to use the resource. COPPA 2.0 also specified the need for education companies to have measures in place to ensure the confidentiality and security of the personal information provided by students. The bill also outlined how companies should clarify their consent procedures for obtaining student information and how they should give information to children and their parents when they request how the company will use the data. The bill was read twice in the Senate and referred to committee, but not enacted (Children and Teens Online Privacy Protection Act, 2019). A similar update to COPPA, known as the Kids PRIVCY Act (H.R. 4801, 2021), was introduced to the House of Representatives in 2021, referred to the Subcommittee on Consumer Protection and Commerce, but ultimately not enacted.

The Kids Online Safety Act (KOSA) is a complimentary bill to COPPA 2.0 and was introduced to the Senate in February 2022 (S. 3663, 2022). It focuses primarily on children's social media use (Hunt-Majer, 2022). The bill would require more options for users to protect their personal information, disable addictive notification features, provide tools for opting out of recommended additional content, and allow parents more control over their children's accounts. The KOSA regulation requires social media companies to perform audits to examine potential harm to their minor users and make their algorithms available to researchers studying the effects of social media use (Bruno et al., 2022; Hunt-Majer, 2022). As of December 2022, the bill has been read twice and referred to the Committee on Commerce, Science, and Transportation (Kids Online Safety Act, 2022).

Student Privacy Laws at the State Level

State lawmakers introduced and enacted a spate of legislation as schools began using third-party companies and systems for education programs, data storage, and analysis. As the use of these systems has grown, hundreds of state student privacy bills have been introduced within the past decade (Data Quality Campaign, 2020a; Student Privacy Compass, n.d.). A Data Quality Campaign (DQC) review found that 241 education data bills were introduced in 41 states in 2020, and 43 were signed into law in 22 states (Data Quality Campaign, 2020a). The increase in state-level education legislation continued into 2021, as 361 bills were introduced in 45 states, and 111 of them were signed into law in 38 states (Data Quality Campaign, 2021).

Student Online Personal Information Protection Act. Most notable of all the state laws was the Student Online Personal Information Protection Act (SOPIPA), enacted in California in 2014 (Russell et al., 2019). This law was the first to prohibit educator websites and vendors from using targeted advertising to students. SOPIPA makes the edtech companies responsible for compliance with the law whether or not those companies had a contract with the school organization. It applies to applications, cloud-based programs, and other online education services. The law does not allow these companies to use personal information for marketing, even if the school agency or the individual student consents. While SOPIPA was the first significant state legislation addressing student data privacy and used a model for other states' legislation, a central critique of the law is that it did not clearly define what "targeted advertising" was (Strickland, 2019). General advertising was still present in some learning program environments based on the users' requests for information or related internet activity. While the SOPIPA legislation has not solved all student data privacy concerns, it has

shifted a significant amount of data protection responsibility to the educational companies providing the resources to education systems.

State Student Privacy Report Card. The lack of comprehensive federal law and lack of clarity on the role of the U.S. Department of Education (Raths, 2016) combined with these disparate state laws were described as a "confusing patchwork of statues" in a report from the Parent Coalition for Student Privacy and the Network for Public Education (Strickland, 2019, p. 1). These organizations created a report card system for each state, published in 2019. The grades for this report (Strickland, 2019) were based on how the student privacy laws in each state address seven key areas:

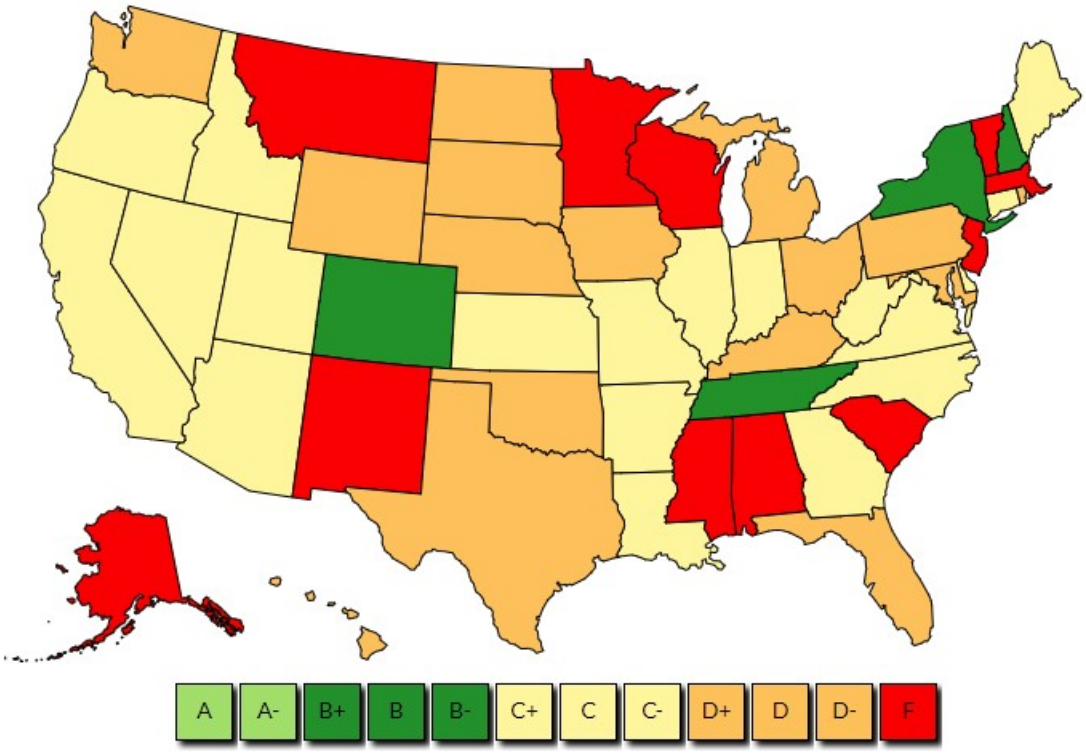
1. Parties covered and regulated
2. Transparency of the regulations in place, especially for parents
3. Parental and student rights beyond the basic rights in FERPA
4. Limitations on the commercial use of data
5. Data security requirements and notifications should breaches occur
6. Oversight, enforcement, and penalties for violations
7. Other provisions that don't fit with the previous grade categories

Each of these categories was weighted depending on how important the organizations believed it was to protect the privacy of student information.

States received a grade in each of the seven areas listed above, and then those weighted grades were combined to create an overall rating (Figure 2; Strickland, 2019). No states received a grade of A, while Colorado, New York, Tennessee, and New Hampshire had a B. There were 19 states which received a C grade, and 17 were at the D level. Finally, there were 11 states which received an F, which includes the state of Wisconsin, the focus of this study. All of the

states with a score of F had 0 points on the rating scale, as none of the states had any state legislation which addresses the privacy and protection of student data (Strickland, 2019).

Figure 2 - Overall Grade, State Student Privacy Report Card



Data Privacy Laws in Wisconsin

Wisconsin is one of eleven states in the country with no state legislation to address protecting student information in online environments specifically. There is general discussion in statute 118.125, titled Pupil Records, about the expectation for the confidentiality of student records. It reads:

> All pupil records maintained by a public school shall be confidential… The school board shall adopt policies to maintain the confidentiality of such records and may adopt policies to promote the disclosure of pupil records and information permitted by law for purposes of school safety (Wis. Stat. § 118.125a).

In essence, the state says schools should keep student records confidential, and districts need to craft their local policies to ensure the safekeeping and appropriate sharing of student information. There is no specific mention of the digital data of students, who make up a significant portion of the state's population.

Within 118.125, pupil *records* are defined as "all records relating to individual pupils maintained by a school" but do not include notes taken during psychological treatment, records from law enforcement, and notes maintained for personal use by a teacher. This section specifies how pupil records can be made available to law enforcement, local health departments, and courts of law. Statute 118.125 also describes how directory information is shared and the expected timeline for schools to notify parents of their procedures for releasing directory information.

While there are no specific policy expectations for Wisconsin school leaders to meet from the state, this also presents a challenge. District leaders are on their own to work with their school boards to research and implement local policies that satisfy federal legislation's requirements regarding student data. As discussed previously, the combination of these federal regulations has challenged education leaders to follow, understand, and seek assistance for enforcement (Anderson, 2022; Electronic Privacy Information Center, 2022; Trainor, 2015; Venzke, 2022).

Wisconsin Student Data System. Statute 115.297 outlines how the statewide student data system is used for cooperative research on school programs with other state agencies in Wisconsin. Within this statute is the requirement for a longitudinal data system that links data from preschool to postsecondary programs. In 115.197(3)(g), it is stated that the agencies using pupil records from the longitudinal data system must "protect student privacy and comply with

laws pertaining to the privacy of student data." The data sharing section of 115.197 provides clear expectations for how data is used, how personally identifiable information is cared for, and how data must be returned or destroyed when no longer needed for the original purpose. These are all key components found in the Data Privacy Pledge, but this section of Wisconsin statutes regulations data sharing among state agencies. The law does not address private companies or other outside organizations that may have student data collected from online data systems or programs. As mentioned above, Wisconsin has no state legislation addressing student data used by third-party companies or organizations using online environments.

Recent Attempts for Wisconsin Student Privacy Legislation. The State Student Privacy Report Card gave the state a grade of F for failing to have any meaningful legislation regarding student data (Strickland, 2019). In August 2016, Electronic Privacy Information Center (EPIC) representatives testified before the state's Legislative Council Study Committee on School Data. They urged lawmakers to go beyond the privacy requirements afforded by the federal Family Educational Rights and Privacy Act (Electronic Privacy Information Center, 2016). A state policy coordinator for EPIC, cautioned the committee on School Data, "Schools and companies collect students' location, health, discipline, social media information, and other sensitive data with no accountability" (EPIC, 2016, p. 2). The suggested privacy solution to the lawmakers was to adopt the Student Privacy Bill of Rights to ensure the privacy of student information in this age of increased digital use in our schools. This committee also heard a presentation from a representative from the National Conference of State Legislatures, who shared examples of student data privacy laws enacted in other states and gave recommendations for what a statute should address in Wisconsin (Wisconsin Legislative Council, 2017).

This work led to the creation of Assembly Bills 71 and 72, introduced in the 2017-18 legislative session and passed out of the Assembly (Wisconsin State Legislature, 2018a, 2018b). Assembly Bill 71 required the State Superintendent's office to create and maintain an inventory of the types of student data collected by the DPI from school districts (Wisconsin Legislative Council, 2017). Assembly Bill 72 required the State Superintendent to provide training and guidance to local districts to ensure compliance with state and federal student data privacy regulations and engage with the public to provide information to share information about student information privacy and security concerns (Wisconsin Legislative Council, 2017). Both AB 71 and 72 passed out of the Assembly, and the Senate's Committee on Education supported them. However, the Senate did not vote on either bill by the end of the 2017-18 legislation session, and the bills failed (Wisconsin State Legislature, 2018c).

Wisconsin Department of Public Instruction Privacy Guidance

The state of Wisconsin has few specific requirements regarding student data privacy in online environments. Still, the state's Department of Public Instruction (DPI) has aggregated a collection of privacy resources on its website for school districts to use to guide their privacy work (Wisconsin Department of Public Instruction, 2022b). The authors of the site recognize the benefits of using data but see the need to balance the use with practices that safeguard the information:

> Using student data for district, school, and classroom improvement planning can be very helpful when it is used correctly and with the necessary security and privacy practices in place. Although data can be used to facilitate change and improvement, there is a need to balance the usefulness of this data with the privacy of the students represented by the

data. Use the following links to become more familiar with Student Data Privacy. (WI DPI, 2022)

The DPI's information about data use and privacy is extensive and informative. Still, it is not intended as a policy for the school districts in the state and does not include a section to guide the work of school leaders.

Wisconsin DPI Privacy Web Resources. The site links dozens of resources created by the federal government, national privacy organizations, and from the DPI itself. The site is organized into six areas: an overview of data privacy, how the DPI safeguards information, privacy information for parents, online training modules for educators, and a collection of resources on student data privacy.

DPI Privacy Training Modules. There DPI provides five training modules: using personally identifiable information, student records and confidentiality, sharing information with other state systems, FERPA, and an online course on data privacy from the Data Quality Campaign. Within the PII training module, there are suggestions for creating and including data privacy policies at the district level. The training on student records describes the different categories of records, how they should be stored and maintained, and how long the district should keep them. This module does not differentiate between traditional paper records kept in filing cabinets and digital records. The training document "Sharing Information Across Systems" was created by the DPI in 2018 and guides sharing information with other community agencies like law enforcement, military recruiters, health care providers, and social workers. The FERPA training module is from the U.S. Department of Education's Privacy Technical Assistance Center (PTAC). This module is a primer to help educators understand the expectations of FERPA. The data privacy training is a self-paced online course from the Data

Quality Campaign and covers the benefits of using data in education, protecting data, basics about data security, and shows how other industries use and safeguard data in digital environments.

DPI Additional Privacy Resources. The resources page contains information for districts, parents, additional training options, and legislation and policy. The information the DPI provides can help individual users and policymakers build their knowledge of privacy issues and link them to model policies and practices used around the country. Like other technology resources in the state, there is no requirement to use these privacy resources. However, the DPI intentionally lets districts know that this information can guide the development of policies and procedures at the local district level. With no student data privacy legislation in Wisconsin, local policies take on even more importance as Bathon (2013a) wrote, "when technology has far outstripped legal theory, the best defense at the local level is robust school policies that have been considered and passed by the school board" (p. 24). Wisconsin district leaders have the challenge of crafting their own data privacy policies. The only regulatory expectations come from a combination of federal laws and the brief mention of pupil records from state statutes.

Educational Organization in Wisconsin

There are 421 Wisconsin public school districts serving nearly 830,000 students in approximately 2200 different schools (Wisconsin Department of Public Instruction, 2022a). Districts range in size of almost 75,000 students in the urban district of Milwaukee, to rural districts with fewer than 100 students in preschool through 12th grade (Wisconsin Department of Public Instruction, 2022a). Annual per pupil spending averages $13,500 across the state, but ranges from $9300 in the rural Slinger district to $18,500 per year in the Nicolet district in suburban Milwaukee (Johnson, 2019). All public school districts in Wisconsin are independent

of one another as no county or regional offices of education regulate the districts within their boundaries. The 12 Cooperative Educational Service Agencies (CESAs) in the state serve as liaisons between the districts and the state Department of Public Instruction. The CESAs provide professional development, program consultation, and grant administration services.

The Department of Public Instruction

The Department of Public Instruction (DPI) is the agency of the Wisconsin government that coordinates and advises the work of public schools in Wisconsin. The agency is led by the, a publicly elected official serving four-year terms. As authorized by Wisconsin Statutes, the State Superintendent leads the DPI and uses administrative rules to direct the department's work and the state's public districts. This rule-creation process is mainly independent of high-level state political activities, as the DPI is not required to obtain the Governor's approval for many of these administrative rules. Instead, rules are drafted within the DPI, approved by the State Superintendent, public hearings are held, and then the rule is sent to the Assembly and State Senate standing committees. All these rules are then published in the Wisconsin Administrative Code. It is from this code register that superintendents and school board members know the legal requirements that must be in place in their district's board policies.

Local School Boards

Wisconsin boards of education are composed of non-partisan elected officials to ensure their school district's academic and fiscal health (Brewer & Picus, 2014). Most board members receive no salary for their work, but it is a small amount if they receive compensation (Brewer & Picus, 2014). The federal government is limited to the powers specified or implied by the U.S. Constitution, and that charter does not mention a system of education. Therefore, the states play the primary role in education as state constitutions typically outline the education system

(Brewer & Picus, 2014). This arrangement means that the state grants district school boards their power, and board members are, in essence, agents of the state.

School Board Authority

Johnson (2013), Shaw (2014), and Baldridge (1995) found local boards generally have the authority to:

- Hire or dismiss the district superintendent
- Create policies for the hiring process of other district personnel
- Negotiate labor agreements with unions and other employee groups
- Levy local property taxes and establish the district budget
- Establish or approve curricular goals
- Oversee the management of district facilities
- Ensure compliance with state and federal legislation
- Investigate, create, and adopt policies not explicitly covered by state and federal laws

Board Policy Creation

The boards execute most of the responsibilities outlined above by developing policies to guide the work needed within the district to satisfy these areas. This is considered the primary activity of a school board, as "In the center of their identity and of proffered reform lies the power of school boards to set policies--and bring life to them--that will form the character of local education" (Baldridge, 1995, p. 60).

When local school boards create policies, a primary responsibility is to ensure district compliance with state and federal laws (Brewer & Picus, 2014). Glass, Bjork, and Brunner (2000) found that most local policies are crafted at the state level or by the district superintendent

and then brought to the local board for approval. Whether local boards create the policies or not, research shows that policy development is a crucial function associated with high-functioning school boards (Danzberger et al., 1994; Goodman, 1997; Johnson, 2013; Land, 2002; LaRocque & Coleman, 1993). Beyond just the development of policies, the highest achieving districts are those whose school boards link those policies to student learning.

School Board Relationship with the Superintendent

Effective boards do not typically make decisions independently, as they must work closely with their superintendent to research, develop, adopt, and revise policies necessary to meet district needs. The board is joined in policy making by the district superintendent, the sole employee selected by the school board (Baldridge, 1995). Johnson's (2013) research found "effective school boards actively connect with district leadership in pursuit of the district's vision and goals in ways that complement the superintendent's implementation efforts" (p. 469). School boards with a positive working relationship with their district leader are likelier to create and adopt policies promoting student learning (Johnson, 2013). Since school boards are often composed of community laypeople, they must have a connection with their superintendent, who typically has years of experience in education practice and training specific to leading education organizations. The role of school boards is not simple, as they "attempt to act as professional organizations, relying on the expertise of the superintendent, and as representative bodies, responding to parent and community demands" (Greene, 1992, p. 220).

When thinking about all that happens in a school district due to the superintendent's work, it is no coincidence that the Association of Wisconsin School Administrators' motto is "Because Leadership Matters" (Association of Wisconsin School Administrators, 2022). The

decisions in these 421 districts come down to the superintendents' recommendations to their board members.

Role of District Leadership

Leadership in educational organizations is a primary factor for school success, especially in making a positive difference in student achievement (Leithwood et al., 2010; Marzano et al., 2005; Waters & Marzano, 2006). Second only to classroom instruction, leadership is the greatest factor in contributing to student learning (Leithwood et al., 2010). School leadership indirectly influences student achievement but directly impacts the staff's actions, especially teachers, within their schools and districts (Leithwood et al., 2010). As stated above, effective board policies are a primary means for outlining school district personnel's philosophies, procedures, and plans. Therefore, the school superintendent working with the board to develop goals and policies is vital for the district leadership team (Waters & Marzano, 2006).

Management and Leadership

Rost (1993) examined school leadership influence and offered his definition as "Leadership is an influence relationship among leaders and followers who intend real changes that reflect their mutual purposes" (p. 102). Rost's work resulted in an analysis of management and leadership concepts. Relationship-building is evident in both categories of district leader activities. Rather than being an influence relationship, management was defined as "an authority relationship between at least one manager and one subordinate who coordinate their activities to produce and sell particular goods and services" (Rost, 1993, p. 145). Rost's *management* is akin to Burn's (1978) *transactional leadership*. Management is a two-way relationship, but primarily it is a top-down arrangement with the manager giving directives to subordinate members of the organization.

While management is a relationship of authority, leadership is one of influence. Management is most frequently a top-down arrangement among managers and subordinates, but leadership is multi-directional and non-hierarchical. Titular leaders can influence followers, but followers can also affect those in leadership or management positions. Regardless of position, leadership means followers can be leaders and vice versa. This concept aligns with distributing, delegating, and developing leadership within a school (Marzano et al., 2005).

Balancing Leadership Styles and Activities. Rost (1993) cautioned not to put leadership and management opposite. Leadership is not the ideal state as compared to management. In the context of schools, leaders need good management skills and practices. Regarding the development of effective board policies, management activities are necessary to ensure they are developed and adopted promptly and accurately. Effective management allows for the structure and systems to be in place for boards and leaders to meet and discuss necessary policy considerations. As principals and superintendents are asked to change and improve practices leading to higher student achievement significantly, they must display Rost's leadership. Leadership activities with school board policy development bring mutual purpose and inspiration to adopt meaningful and necessary policies. Once new policies are in place, both management and leadership actions are essential to help the rest of the district staff understand, accept, and do the work needed to bring the policies to fruition.

Other scholars have similarly examined Burns's work with transformational and transactional leadership within schools (Bjork & Gurley, 2003; Pepper, 2010). This research found that school leaders can not only rely on skills traditionally associated with transformational leadership. School leaders must inspire staff, a transformational activity, to change their instructional methods. However, transactional skills are also required to meet the

expectations of school reform in the era of accountability. Transactional duties like student discipline, establishing staff rules and routines, and coordinating schedules can positively affect creating a stable and predictable school environment (Pepper, 2010). As important as it is to inspire staff and students to reach high levels of learning and change, it is also essential to ensure that systems are in place to provide consistency and stability once those changes have happened. When transactional skills support transformational leadership techniques, there are positive effects on the school organization (Bjork & Gurley, 2003).

Waters and Marzano (2006) identified several district-level leadership responsibilities and actions related to goal setting correlated with student achievement. The first is that superintendents should include various stakeholders from the district when setting goals. This work is aligned with transformational leadership activities as they attend to the needs and interests of the people within the organization (Burns, 1978). Selecting non-negotiable goals for student achievement and instructional methods is the second area for effective goal setting. Finally, the superintendent's activities can be classified as transformational when the leader inspires the school community to accept and work toward these goals. A transactional approach like employee discipline could also be used to make sure staff members are working toward these goals.

Another district leadership responsibility for goal setting is working with the school board to support the goals (Waters & Marzano, 2006). A transactional activity like factual communication would help share goal information with the school board. The next effective responsibility of the superintendent is monitoring the achievement and instructional goals. Again, this is mainly transactional work to see that all the efforts within the district fall in line with the previously set goals and policies, using rewards and punishments as needed.

Superintendent's Work with School Boards

Working with the board would necessitate transformational actions if the superintendent needed to influence or inspire board members to understand, adopt, and support these goals. This is especially necessary as there is frequent conflict among board members within the community and in the relationship between the board and superintendent (Bjork & Lindle, 2001). Superintendents may need to act as political strategists, professional advisers, decision-makers, or all three, depending on the specific situation of the community and board environment (Bjork & Lindle, 2001). The complexity of policy creation and adoption was evident in Kingdon's (2003) framework to understand how policy streams, problems, and politics influence the process. In addition to understanding the policies at hand and the players involved, school leaders must also be aware of the policy implementation process. A policy's impact depends on the local context, the influences of the players involved, the complexity of the policy itself, and the inevitable adaptations that occur as part of the implementation process (Young & Lewis, 2015).

District Leadership Summary. The leadership displayed by superintendents is vital for students' success in schools. Transactional and transformational leadership practices are necessary to ensure the district has the appropriate culture and systems to support student learning. In addition, district leaders need to manage and lead in their relationships with other school community members to meet district goals for their students. These leadership styles and practices are also required when superintendents work with school boards to implement policies and resources to support the staff and students.

District-Level Technology Leadership

As with district-level leadership on student achievement, leadership is vital for successfully implementing and using technology within schools (Anderson & Dexter, 2005; Bjork, 1993; Levin & Schrum, 2012; McLeod et al., 2015). This is especially true as superintendents play the roles of adviser, strategist, and decision-maker while working with the school board. Individual teachers, students, and other school stakeholders are becoming more adept at using technology resources. Still, it requires the work of the organization's leader to make sure technology use is done intentionally and systematically to lead to real change and progress for the school (Sessum in McLeod et al., 2012). Effective technology implementation in schools requires the work of school leaders, especially superintendents, to make that change happen. McLeod et al. (2011) stated:

> Whether it be wireless infrastructure, student device deployment, policy revision, teacher training, or other key aspects of technology integration, the superintendent's traditional instructional leadership role takes new forms when confronted with digital learning tools, campus networks, social media, and other online systems (p. 105).

Good Technology Leadership is Good Leadership

As educational technology use grew after No Child Left Behind, research showed that "good technology leadership is essentially just good leadership for our digital, global era" (Richardson et al., 2015). As with any instructional movement, school leaders must be primary players in integrating technology tools in district classrooms (Anderson & Dexter, 2005; Dexter & Richardson, 2020; Sauers et al., 2014). When superintendents use their leadership position and focus on relationships within their district, they prime technology to be used innovatively (Richardson & Sterrett, 2018).

Dispositions of Effective Technology Leadership

Dexter and Richardson (2020) identified critical leadership dispositions in effective technology leadership. These leaders developed a vision for the district and the use of relevant technology for a connected digital world. Leaders also collaborated with the various school community members and supported the collaboration among their teaching staff. They set clear forward-sighted expectations for instruction and the use of technology in the district. Effective technology leaders also saw the change process as centered on the needs of individuals in the school district, not just on the technology itself. Superintendents seen as influential technology leaders also took appropriate risks and motivated teachers and students in their schools (Richardson et al., 2015). These leaders also learned with their teachers how to use the technology tools they advocate for. All these dispositions were vital for the role of the superintendent as a learning leader and were present within their leadership of technology use in schools (Richardson et al., 2015). Research also shows that superintendents should prioritize infrastructure, communicate effectively, and provide appropriate professional development for the teaching staff (Richardson & Sterrett, 2018; Sauers et al., 2014).

Data Privacy Leadership

Hitt and Tucker's (2016) framework for leadership practices and student achievement does not explicitly address student data privacy. However, privacy leadership would be applicable within the domains *establishing and conveying the vision*, *facilitating a high-quality learning experience for students*, and *connecting with external partners*. Using data for continual improvement is a dimension within the vision domain, and leaders should address student data privacy and security as part of the effective use of data systems. Modeling ethical practices is another dimension within the vision domain, and the safekeeping of personal information can be

seen as an ethical issue (Lee et al., 2016). External accountability is also found within the vision domain, and school staff are responsible for complying with federal and state regulations and parent expectations regarding the appropriate use and security of student data. Effective leaders give context to these outside requirements and develop goals and practices to meet the expectations (Hitt & Tucker, 2016). Leading data privacy efforts would fit within the dimension of maintaining safety and orderliness in Hitt and Tucker's (2016) domain for facilitating a high-quality learning experience for students. School leaders can create, enforce, and monitor policies and practices to ensure a safe environment for using technology resources and student information. Within this framework, effective leadership practices include communicating and building relationships with families in the domain of connecting with external partners. School leaders can communicate with parents on how student data is used within learning programs and services and share the practices in place to protect personal information about the students.

National education organizations have also expressed the role of school leaders regarding the privacy and security of student data. The National Association of Secondary School Principals (2022) provides a list of recommendations for district and building-level leaders to effectively and appropriately use student data. For district leaders, these include creating information inventory policies about what data is collected, how it is used, and how it is safely secured. District leaders also need to ensure contracts with third-party education vendors address the use of their students' information and establish vetting procedures for procuring new technology resources. These leaders are also responsible for training district staff members to understand applicable policies and governmental regulations and use practices that meet this guidance's expectations. The NASSP recommends that building leaders are familiar with all applicable federal, state, and district regulations and then communicate the relevant policies and

roles to school staff and parents. Building-level leaders are also responsible for ensuring staff compliance with these policies and subsequent training (National Association of Secondary School Principals, 2022).

The American Association of School Administrators (AASA) recognizes the importance of technology and its role in enhancing learning environments. Still, it does not explicitly mention student data privacy within its organization's position statements (American Association of School Administrators, 2022). However, AASA partnered with the Future of Privacy Forum to produce the Policymaker's Guide for Student Privacy (Future of Privacy Forum, 2019). This guide is intended to help create federal, state, and local data privacy policies. It recognizes school district leaders' important perspective in knowing their organizations' needs and the gaps within federal and state privacy regulations. The AASA partnered with the FPF again in 2020 to release a white paper to guide school leaders and policymakers on student data issues relating to the COVID-19 pandemic (Student Privacy Compass, 2020a).

The AASA is a member of the National Policy Board for Educational Administration (NPBEA), which publishes the Professional Standards for Educational Leaders (NPBEA, 2015). These leadership standards were last updated in 2015 and make a brief general reference to student data. The policy states that effective leaders "Develop technically appropriate systems of data collection, management, analysis, and use, connecting as needed to the district office and external partners for support in planning, implementation, monitoring, feedback, and evaluation," (NPBEA, 2015, p. 18).

The Future Ready Schools initiative provides a framework for school district leaders for best practices in student data privacy (Alliance for Excellent Education, 2022). This framework posits that district-level leaders support student-centered learning in the area of data and privacy

through implementing and communicating district policies that adhere to state and federal laws and ensure high levels of student information privacy and security. The USDOE's Privacy Technical Assistance Center (PTAC) calls on district leaders to provide intentional privacy and security training to all staff members to ensure student data's safekeeping and appropriate use (U.S. Department of Education, 2015).

ISTE Standards for Education Leaders

Like the research outlined above, the Standards for Education Leaders from the International Society for Technology Education (ISTE) suggest leaders can develop and promote a vision, empower staff through professional development, focus on infrastructure, and model learning themselves through the acquisition of knowledge and use of digital tools (International Society for Technology Education, 2022). The ISTE standards also urge school leaders to advocate for equity and citizenship, where they look at issues like student access to technology tools and model appropriate digital use. These standards also directly address policy insight for school leaders in the legal use of technology, protecting the privacy and security of student information, and ensuring staff members observe privacy and data management policies. Standard 4c recommends that school leaders:

> Protect information and data through precautionary planning and actions, such as training to establish and maintain best practices among staff and students, complying with state and federal regulations for protecting student data and privacy, and choosing technology products and vendors that have robust privacy policies and security capabilities (ISTE, 2022, section 4c).

The ISTE standards specifically address data privacy for students, educators, and education leaders. As digital citizens, students are expected to "manage their personal data to

maintain digital privacy and security and are aware of data-collection technology used to track their navigation online" (ISTE, 2022, p. 3). The standards also ask educators to model using and managing personal information and digital data to protect students' privacy. For school leaders, the expectations for ensuring student data privacy are outlined in the role of Systems Designer. That standard states leaders are to "Protect privacy and security by ensuring the students and staff observe effective privacy and data management policies," (ISTE, 2022, p. 8).

Technology Leadership with School Boards

There is a lack of literature on how superintendents work with school boards to understand and implement technology policies (McLeod et al., 2011). Still, Richardson and Sterrett (2018) found as technology use became more commonplace in districts, superintendents recognized the need to change and adopt district policies that ensured the appropriate infrastructure and funding were in place to support effective technology use in their districts. While there is little research on the topic of superintendents understanding and guiding student data privacy policies, this author believes the previously described skills and dispositions of a technology leader would be an asset for superintendents working with school boards for the adoption of such policies. In addition to creating district privacy policies, school leaders are responsible for ensuring the successful execution of those policies. Leaders also need to establish procedures and practices which lead to the fulfillment of the policies adopted to ensure the privacy and security of student data.

Technology Leadership Summary

Leadership matters when it comes to the successful use of technology in schools. Effective superintendents and school leaders successfully lead technology use and integration when they set a vision paired with expectations, work collaboratively, focus on individual staff

needs for professional development, take appropriate risks, and be a learner with the technology tools they promote. Successful superintendents also support technology by attending to the infrastructure and organizational processes, serving as student advocates for access, and ensuring there are policies in place for the legal use of tools and the protection of student information.

Conclusion

Research on the definitions and concepts of privacy vary widely, as do federal and state laws and regulations on student data privacy. There is a lack of scholarship on policies addressing student data privacy at the local school board level, so this will continue to be a need for the appropriate balance of educational technology and the privacy and protection of student information. Uses of educational technology which rely on digital student information have grown dramatically in the last 20 years and will likely continue to be an essential tool for educators and schools. School boards and school leaders must work together to ensure adequate policies to address this issue. School superintendents must ensure they are knowledgeable about appropriate technology privacy policies and the other attributes correlated with effective technology leadership. Not only do the district leaders need to have the appropriate level of knowledge for policy creation, but they should also effectively implement the policies by establishing procedures and practices and identifying which school district members are responsible for carrying out these actions. Understanding how current board policies in Wisconsin address student data privacy and federal laws will help position current and future school leaders to make the best use of educational technology tools while protecting students' privacy.

CHAPTER 3: METHODOLOGY

As described in Chapter 2, schools increasingly use developing technology resources and tools while educating students. These tools serve many purposes, including professional development, communication with stakeholders, student instruction, and the storage and analysis of student information. The power and complexity of these digital tools keep growing, which benefits many school district responsibilities and processes. Still, it does represent a challenge for school personnel to govern access to student information. Many of the digital services used by schools utilize third-party vendors, cloud storage, and other platforms which store district data outside the direct control of district personnel. While there are obvious benefits to using student data in digital environments, school officials must take caution so the data is not misused, inappropriately shared, or compromised through illegal access.

As outlined in Chapter 2, federal regulations guide the appropriate use of student data. Still, there are gaps between the laws and how they are implemented at the local school district level. In Wisconsin, the regulatory guidance is not detailed or clearly defined. Therefore, each school district implements its district policies to direct the practices on how student data is collected, stored, and shared. The superintendent and other education leaders work with the school board to draft and adopt policies to guide this work with technology use and how student information is used.

The purpose of this study was to understand how school board policies in the state of Wisconsin address the privacy of student data. In this chapter, I identify the research questions for the study and then go into detail to explain the research design. I include an explanation of the analytical choices and procedural decisions used to understand how district policies address the privacy of student data and how those policies address federal regulations.

Research Questions

To understand student data policies in this study, I followed three research questions to guide my inquiry.

1. How is student data privacy protection addressed in the student records sections of school board policies in public school districts in CESA 4 in Wisconsin?
2. How do these local policies address federal student privacy obligations?
3. Who do these policies task with leading and managing the implementation of student data privacy policy?

I use the first research question to gain an overall understanding of how school districts describe their procedures for addressing the use of student information. The second question was postulated to understand how the district policies specifically addressed the federal regulations of FERPA, COPPA, and PPRA. Finally, the last research question helped specify who is designated to lead and manage the student data privacy policies through these board policies.

Research Design

I used a qualitative approach to answer the three research questions. The questions necessitated an analytical approach to understand what language and guiding practices were present in existing school board policy books. I used the qualitative method, document analysis, to explore these questions.

Document Analysis

Document analysis is a qualitative approach to studying and assessing documents (Bowen, 2009; Prior, 2003). This approach often involves interpretation by the researcher that gives meaning to the document being studied. It is one method to help understand the people or organization that produced the record. In addition, document analysis can provide more

information about the typically unobservable activities of an organization and information to understand the more public activities of that institution (Hatch, 2002). The use of documents is also an essential means of understanding past events, especially when there may be no other sources of data remaining (Bowen, 2009).

The use of documents can be the sole method for collecting and analyzing information about a phenomenon, but DA is often used in conjunction with other qualitative methods like case studies and interviews (Bowen, 2009; Hatch, 2002; Maxwell, 2013; Merriam, 2009; Owen, 2014; Wesley, 2010). The data collected from documents is analyzed like other qualitative approaches (Bowen, 2009; Merriam, 2009).

Documents are a plentiful data source and are considered anything that existed before the research began (Bowen, 2009; Merriam, 2009). Some common examples include personal letters, maps, songs, financial records, government documents, and music. Governments and other bureaucratic organizations create large amounts of documents, which can be excellent data sources for understanding the institutions that produce them. In addition, documents can be used to understand the actions and processes the researcher cannot observe. This non-observation can be due to the nature of the action, the time when the event occurred, or the location in which it occurred (Merriam, 2009; Prior, 2003).

I used school board policy documents as my only data source for this research. I made this decision because of the nature of board policies compared to other qualitative research documents. As explained in Chapter 2, policy creation is one of the primary responsibilities of a local school board. Elected school board members represent the community, and the policies they create and adopt establish philosophies and procedures for how the district will provide educational services for the students. In essence, these board policies are democratic statements

from the community. The protection of student data within public schools can be studied in myriad ways, and the focus on policies is a means to understand the school board's intentions.

Since these policy documents are my only data source, I relied solely on document analysis as the methodology for understanding what exists within these policies. One could broaden the understanding of these policies through interviews with those who created the policies or examine how school board members implement the policies. Still, my intention with this study was to establish a deep understanding of the content within the policies.

Guidance for Using Documents

Prior (2003) provides key concepts to consider when using documents for research. First, it is essential to understand the context in which the document was created. Documents are social products, so the researcher should know who produced them and why. Researchers who use documents as part of their work should know the purpose the document was created to serve (Prior, 2003). When analyzing school board policies, the researcher needs to know that those policies are designed to guide the actions of the employees, students, and other school district members.

Wesley (2010) guides researchers in using DA to ensure their work's highest trustworthiness and legitimacy. First, those using DA must protect the authenticity of their research by providing the reader a plausible interpretation of the document. This is accomplished by providing great detail about the analysis process so the reader understands how the researcher came to their conclusion. The second concern is the portability of research using DA. Are the findings of the study relevant beyond the specific case being examined? In quantitative terms, this is known as generalizability. The subsequent guidance is to consider the precision of the analysis of the documents (Wesley, 2010). This analysis could be considered precise if another

researcher could reach the same conclusions had they read and analyzed the same document under similar circumstances. Finally, researchers must be cautious with the impartiality of their work with data in documents. Researchers should show that the conclusions derived from the documents are free from their own biases and beliefs. Following all these suggestions will help qualitative researchers using DA avoid criticisms about the quality of their work as compared to those using quantitative means. Providing extensive detail about the data collection and analysis techniques helps show thorough quality work when using document analysis (Bowen, 2009).

Data Collection Using Documents

The data collection procedures for qualitative research depend on the data source (Creswell, 2009; Hatch, 2002; Merriam, 2009). There are several procedural requirements and social norms to follow for collecting data through interviews with and observations of people. Still, unobtrusive sources like documents are typically not as complicated or time-consuming (Hatch, 2002). For personal communication documents like letters and emails, it is often necessary to obtain the permission of the document's creator before using it for research. There are few requirements for collecting and using many publicly available documents created by governmental agencies. When using government documents that require permission, the researcher should carefully follow the requirements for the care and use of those materials (Hatch, 2002). Documents containing sensitive information, like health records or student discipline information, should be stored safely and securely so the information is not shared with those who don't have permission to view it.

Document analysis has been used in recent studies to examine federal and state laws in addition to the policies of local education organizations (Ham, 2021; Lim et al., 2021; Mordecai, 2022; Welton & Freelon, 2018). Ham's (2021) research relied on document analysis to explore

how universities developed policies and procedures and whether they addressed ethical issues using data analytics and student information. This research concluded with recommendations for university leaders to examine their policies and involve students in policy-making when the students' data was being used. Similarly, document analysis of records retention policies was used to help understand the use of learning analytics programs at a Malaysian university (Lim et al., 2021). The research conclusion suggested that university leaders further involve those in middle management to understand the guiding policies and then develop internal practices for enforcing these overarching policies. Mordecai's research (2022) on balancing student privacy and innovation in a K-12 school district used DA to examine state and federal laws, federal publications guiding educational technology use, and school district policies. Welton and Freelon (2018) employed document analysis to understand how community leaders reacted to and eventually influenced district board policies regarding school closures. In a more general sense, Cardno (2018) delved into how document analysis is used not only as a research method but also as an educational leadership tool to help leaders understand the policy's purpose and competently implement actions to satisfy the policy's requirements.

Data Analysis from Documents

The data analysis for documents is similar to the processes used for other qualitative approaches. Generally, the analysis is an iterative and inductive process where the researcher repeatedly reads, codes, categorizes, interprets, and explains what is found within the documents (Bowen, 2009). As with other qualitative approaches, there are many ways to make sense and meaning of the data, but Bowen (2009) suggests that thematic analysis is a method that applies to many types of analysis for documents. After an initial review of the documents, the reviewer

looks closer at coding the data into different categories. Then, the researcher can begin finding themes within the data related to the research goals from those categories.

Wesley's (2014) description of using document analysis in political science is similar. First, the researcher conducts a broad review of the documents and uses an open coding approach to understand what is in the documents. The second step is another review of the data to employ an axial coding technique to assign themes to all the coded data in the first round of analysis. These two steps are like Bowen's (2009) work, but Wesley (2014) adds a third selective coding stage to intentionally look for tagged passages that were miscoded or find data bits that are discrepant and not fitting with previously identified themes.

While not strictly an analytical method for research using documents, typological analysis, as described by Hatch (2002), is appropriate for a study about data privacy in public school district policy books. In this approach, the researcher uses predetermined typologies to categorize the data found within the documents instead of inductively discovering the categories. These typologies can come from the research objectives, common knowledge about the topic, or concepts described in theoretical frameworks. Before beginning this type of analysis, the researcher needs to know the typologies well to justify why the information in the documents fits with that typology. Hatch (2002) recommends that the researcher begins the work by having only one of the predetermined typologies in mind as they read, noting only the passages that are related to that typology. This process is repeated for each conceptual type until all the data related to the typologies has been identified. Passages will likely be categorized under multiple typologies. The next phase of the analysis is looking for patterns, relationships, and themes within each typology. At this point, the researcher should examine those patterns

and themes to see if they make sense within the conceptual framework used to create the typologies. Does the data support the hypotheses formed within that framework?

Theoretical Framework

A review of methodological research recommends that academic research utilize a theoretical or conceptual framework to help guide the methodological design (Creswell, 2009; Hatch, 2002; Merriam, 2009). This study used contextual integrity (CI) as the framework to help understand how board policies address student data privacy in schools in Wisconsin (Nissenbaum, 2010). This privacy concept focuses on the social structures or contexts where information flows from one agent to another. Context, actors, attributes, and transmission principles are key aspects of contextual integrity. The contexts are the situations in which information is shared. Actors are the people who send, receive, or produce the information shared. Attributes refer to the type of information shared. Transmission principles are the conditions in which the information should or should not be transferred. The system has integrity when the actors follow the context norms for the flow of information from one actor to another with the appropriate transmission principle. These four CI concepts will be my initial starting point for coding and organizing the data in the school board policies.

School leaders are influential in all aspects of the flow of student information within their school districts. They are key players in creating and adopting the policies that are formal norms in the CI framework. Leaders are also influential with informal norms like school culture and how the culture emphasizes the care of students and their sensitive personal and educational information. Leaders create and monitor their employees' procedures and practices, which regulate how and what information is shared. These stated expectations are also considered norms, and the activities specified by the procedural guidelines would be regarded as the

transmission principles in the framework. Beyond creating and enforcing school norms and data transmission principles, school leaders are also essential actors in the Contextual Information framework as they send and receive information about students with other members of the education context.

Data Sources

This study aimed to understand how school board policies address student data privacy. Board policies are the documents that guide the actions of school district employees as they execute their obligation to provide education to students who live within their district boundaries (Wisconsin State Legislature § 121-02). Documents like board policies are excellent sources of information to understand an organization's operations and value systems (Hatch, 2002; Prior, 2003). School board policies address nearly every aspect of the operation of the district, and the sections of the policy books devoted to student records will be the focus of this study to answer the research questions.

Student Records

To understand generally what a student record is, Wisconsin State Statute 118.125(e) states, "Record means any material on which written, drawn, printed, spoken, visual, or electromagnetic information is recorded or persevered, regardless of physical form or characteristics." This same statute also provides general descriptions of three different types of student records. First*, progress records* involve information about grades, attendance, courses taken, extracurricular activities, immunizations, and lead screening. The category *behavior records* is broad and include results of group and individual tests, discipline information, law enforcement and child welfare, and other pupil records that are not considered in the progress records category. *Patient health care records* are the last category outlined by state statute. This

information concerns the student's health and is usually provided by a student's healthcare provider with the consent of the student's parents for use in a school evaluation to determine if and how the student's health may impact their learning.

District Student Records Policies

Typically, district policies address a range of procedures for student records according to the direction from 118.125(2), which states "The school board shall adopt policies to maintain the confidentiality of such records and may adopt policies to promote the disclosure of pupil records and information permitted by law for purposes of school safety." They can determine who has access to student information, how it should be stored, and to whom the information can be disclosed. These policies can also guide how long records are retained, to whom they can be transferred, and when the information can be destroyed (Wisconsin Department of Public Instruction, 2022b). Based on the state definitions of student records and how district policies are asked to address records, it is logical to use the student records sections of specific district policy books to address the two research questions for this study.

Study Population

This study examined the student records policies for the public school districts found within Cooperative Educational Service Agency 4 (CESA 4) in Wisconsin. There are 12 CESAs in the state, and they are regional governmental agencies that serve as the liaison between the member school districts and the state's Department of Public Instruction. These agencies provide services to their member districts like professional development, shared teachers, program consultation, cooperative purchasing, and grant administration. These regional agencies serve the unique needs of their member district. Each CESA is governed, through policy and

budget development, by a Board of Control, composed of professional personnel from the districts they serve (CESA 4, 2021).

I chose CESA 4 for this study because its member districts are representative of the types of school districts found in Western Wisconsin and similar to the state demographics as a whole. There are 26 K-12 school districts in this region which serve over 35,000 students from 9 Wisconsin counties (CESA 4, 2021). Table 2 lists the districts within CESA 4. The schools within these 26 districts serve students who live in urban, suburban, and rural communities. Looking at the state, 14% of students have a disability, 44% are economically disadvantaged, and 69% are white (Wisconsin Department of Public Instruction, 2022a). Collectively, 14.4% of the students in the CESA 4 districts have a disability, 45% are economically disadvantaged, and 79% are white. Another reason I selected this regional agency because I have worked in two of the member districts and have personal and professional connections that aided me in checking my data collection, analysis, and findings.

Table 2 - CESA 4 District Demographic Data

District Name	Enrollment	Economically disadvantaged	With disability	White
Alma	240	42%	18%	93%
Alma Center Humbird Merrillan	601	64%	12%	81%
Arcadia	1257	78%	9%	24%
Bangor	597	33%	9%	93%
Black River Falls	1654	61%	17%	66%
Blair Taylor	597	46%	17%	91%
Cashton	625	40%	15%	87%
Cochrane- Fountain City	562	33%	11%	91%
Desoto	490	50%	19%	94%

Gale-Ettrick-Trempealeau	1377	30%	13%	90%
Hillsboro	533	50%	15%	90%
Holmen	3855	23%	12%	86%
Independence	386	71%	13%	49%
La Crosse	6269	52%	15%	69%
La Farge	230	64%	18%	93%
Melrose-Mindoro	748	90%	17%	90%
Norwalk-Ontario-Wilton	605	61%	17%	79%
Onalaska	3056	30%	12%	74%
Royall	489	60%	15%	91%
Sparta	2908	53%	17%	78%
Tomah	3041	40%	18%	84%
Viroqua	1057	42%	12%	93%
West Salem	1782	30%	13%	93%
Westby	1044	37%	14%	94%
Whitehall	748	50%	13%	82%
Wonewoc-Union Center	335	56%	15%	92%
CESA 4 total	35086	45%	14%	79%
State total	829935	44%	14%	68%

Data Collection

District policy books are public records in Wisconsin, and school districts choose how these documents are made available to the public. In CESA 4, 20 districts had full policy books available online (Table 3). Of the districts with their policy books online, 15 use an organization and storage service called BoardDocs to make their policies available. These districts linked the policies from the district web pages to their policy books at BoardDocs. Twelve districts had their BoardDocs links posted on their district web page. Four districts had their policy books published online but did not use the BoardDocs service.

Table 3 - Policy Access of CESA 4 Districts

Host Method	Number of districts
BoardDocs site on district page	15
Local method	5
Policies emailed on request	5
Policies not provided	1

For the six districts that did not post their policies online, I emailed the districts' superintendents requesting digital copies of their policy books. The public records law in Wisconsin states that the requester of records does not need to give a reason for the request. Still, I did share with the superintendents that I was using their policies as part of a doctoral research project through the University of Kentucky.

Two of those superintendents, from Westby and Hillsboro, emailed me links to their BoardDocs sites which were not listed on their district pages. The Desoto district also used the BoardDocs service, but the administrative assistant I emailed with did not send me the link to their platform. However, this staff member emailed me all the policy sections I requested. The superintendents or administrative assistants from the Independence and Whitehall districts sent me copies of policy sections related to student records and the maintenance of student data. The school district of Melrose-Mindoro was the only district in CESA 4 that did not send policies in response to my request. The administrative assistant I emailed said their policy book was not in a format where she could quickly email it.

To find the relevant policy sections for policy books hosted in the BoardDocs platform, I used the service's search tool to locate the policies labeled *student records. Next,* I downloaded those sections as PDFs and uploaded the documents as text files to Dedoose, a computer-aided qualitative analysis application. I started with the policy sections titled *student records* and then

found other policy sections referenced in the student records policies that seemed relevant to this study.

I used a similar process for the four districts which did not use BoardDocs to organize and display their policies. I located the policy sections for student records and found other policies referenced within the records sections. All these policies were converted to text files and uploaded to Dedoose for further analysis.

The policy collection process occurred within the same two-week window of October 2022. As Hatch (2002) recommended, I kept notes about my policy collection activities in a researcher's log. I noted the dates I downloaded the policies from the district service, the dates I emailed the superintendents, and the dates the policies were emailed back to me.

Data Analysis

To derive meaning from these policy documents, I followed the work of several methodological scholars (Bowen, 2009; Creswell, 2009; Hatch, 2002; Merriam, 2009; Owen, 2014) by consolidating and organizing smaller pieces of data to help understand larger themes from the information in these school policy documents. The first review of the policies was a superficial examination to get an overall sense of the document organization and to find sections relevant and meaningful to the research questions (Bowen, 2009).

The following analysis phase was a closer reading of the policies with specific concepts in mind (Table 4). Since this study was guided primarily by the privacy framework, *contextual integrity*, I utilized the typological analysis approach described by Hatch (2002). To find relevant sections to address the first research question (RQ1), I used the search and tagging feature of Dedoose to find general terms like *privacy, security, records, confidentiality,* and *personally identifiable information*. Then, I coded each of these occurrences within all of the

documents. For RQ2, I followed the same process to search and tag terms for the federal regulations relevant to the collection, storage, maintenance, and disclosure of student data. These regulations are the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Protection of Pupil Rights Amendment (PPRA). With RQ3, I searched and tagged the occurrences of school personnel mentioned in each policy, with the initial emphasis on the roles of superintendents, principals, and technology directors. As Hatch (2002) recommended, I used an iterative process for these first analysis phases. I searched for one typology at a time, tagging all these passages in the Dedoose before moving on to the next review stage for a different term.

Table 4 - A Priori Codes

Nissenbaum's Contextual Integrity		
Contexts Classroom District-wide Family Nested contexts Actors Senders of information Recipients Information subjects	Roles School staff (teacher, administrator, board member, etc.) Parents Students Military recruiter College recruiter Law enforcement No actor specified	Norms Federal regulations State regulations
Attributes (information types) Student PHI Student PII Education records Directory data	Transmission principles Disclosure Restricted access Confidentiality Parent consent No parent consent Notification Marketing of information	Activities Record retention Record sharing Service subscriptions
Federal student privacy regulations FERPA COPPA CIPA PPRA		

Subsequent rounds of searching and coding were based on the Nissenbaum (2010) framework of *contextual integrity*, which examines privacy in terms of the flow of information in a given context. With the CI concept of *roles*, I coded occurrences of students, parents, school staff, and third parties like college and military recruiters and assessment companies. I also coded the CI concept of *actors*, noting if any people in the previously mentioned roles were the senders or receivers of information. I coded the occurrences of information *attributes* like

education records, personally identifiable information, personal health information, and directory data. Data-sharing *activities* were found and coded for data collection, storage, and disclosure. I also searched and tagged the *contexts* or situations in which information flowed. Examples of these contexts are transferring student records to other districts, sharing student data for compliance activities with the state Department of Public Instruction, collecting student data in surveys, and disclosing student information for assessment and instructional services. I also found and coded the various *transmission principles* which are part of the flow of student information and described the expectations or restrictions for how and if data is shared. These transmission principles were present regarding parental consent and which types of information could be shared in the given context of the information flow.

As Creswell (2009) recommended, I was also open to adding additional codes that emerged during the coding and analysis phases of the research. As a result, I discovered and coded concepts I did not initially anticipate, including sharing student data in emergencies, working with law enforcement, additional relevant state regulations, and school board philosophical support statements for using technology. These additional concepts are detailed in the results section of this study.

Throughout these first rounds of searching and coding, I used memo writing to document my initial thoughts, interpretations, and hunches about what was present within the policy documents (Bowen, 2009; Hatch, 2002; Owen, 2014). These memos also ensured consistency with analysis and coding from one policy document to the next. For example, I would note a particular theme or concept found within one document, and then use the memo to describe what to look for in other sections.

After these initial cycles of coding and tagging individual terms as described above, I then reviewed each policy document. Next, I created excerpts of the sections, applying each individual code to that larger excerpt. When making these excerpts, I also referred to the original policy document I downloaded from the district to ensure I looked at each excerpt within the original context. After each document was excerpted and coded, I looked for patterns, emergent themes, and relationships within and among the policies (Hatch, 2002). I frequently referred to the contextual integrity framework and federal regulations to see if these emergent themes made sense with these concepts.

Role of the Researcher

Data collection and analysis in qualitative research necessitates the researcher to serve as the primary data collection tool (Creswell, 2009). While there was no live observation of human participants in this study, I was the primary observer of the data sources used to understand the research questions posed at the study's outset. I collected the policy documents from the school districts within a regional education service agency in Wisconsin, where I live. I live within one of these school districts, and my children both attended public schools in two of these districts. I worked as a principal for a total of 16 years in two of the districts in this study. I am no longer a school district employee, but I still have many friends who work within these districts. Several friends work as school leaders; others serve on the school boards that create, adopt, and implement the policies.

While I have close connections within many of these school districts, I did not exclude the data from these districts because of the nature of the board policy creation and adoption process and my lack of influence and communication about these policies. My past participation in policy creation occurred more than five years ago. My previous participation enabled me to

have familiarity with district policy processes and is beneficial to my role as primary observer and analyzer of these policy documents.

Additionally, I am a proponent of the appropriate use of student data as a resource in the effective use of educational technology. My experience as a school administrator who embraced school technology likely influenced my perceptions of policies and the required procedures.

Conclusion

This chapter explains the methodological considerations which were used to develop the study to understand how the 26 public school districts in CESA 4 of Wisconsin address student data privacy within their board policies. It began with a description of the qualitative methodological approach, document analysis, and how it is appropriate to understand how school board policies address student data privacy. This is followed by the description of Nissenbaum's (2010) privacy framework *contextual integrity* and how it is used to understand the flow of information in given contexts. The next portion of this chapter explained the school district policies' choice and how those policy documents were collected and analyzed. Finally, the chapter concluded with the researcher's role in the study's planning and conduction. The following chapter presents the results, organized by the three research questions guiding the study.

CHAPTER 4: FINDINGS

This study examined how public school districts in Wisconsin's Cooperative Education Service Agency 4 (CESA 4) address student data privacy within their board policies. To accomplish this, I have used the qualitative methodological approach of document analysis to understand the procedures and expectations expressed in the policy books of these districts. In this chapter, I present the findings of the analysis of these policy documents with attention to the general approach of student data privacy within student records policies, how the policies address federal regulations, and the role of school leaders in implementing these policies.

The research questions posed at the beginning of this study guided the methodological approach outlined in the previous chapter. The three questions for this study were:

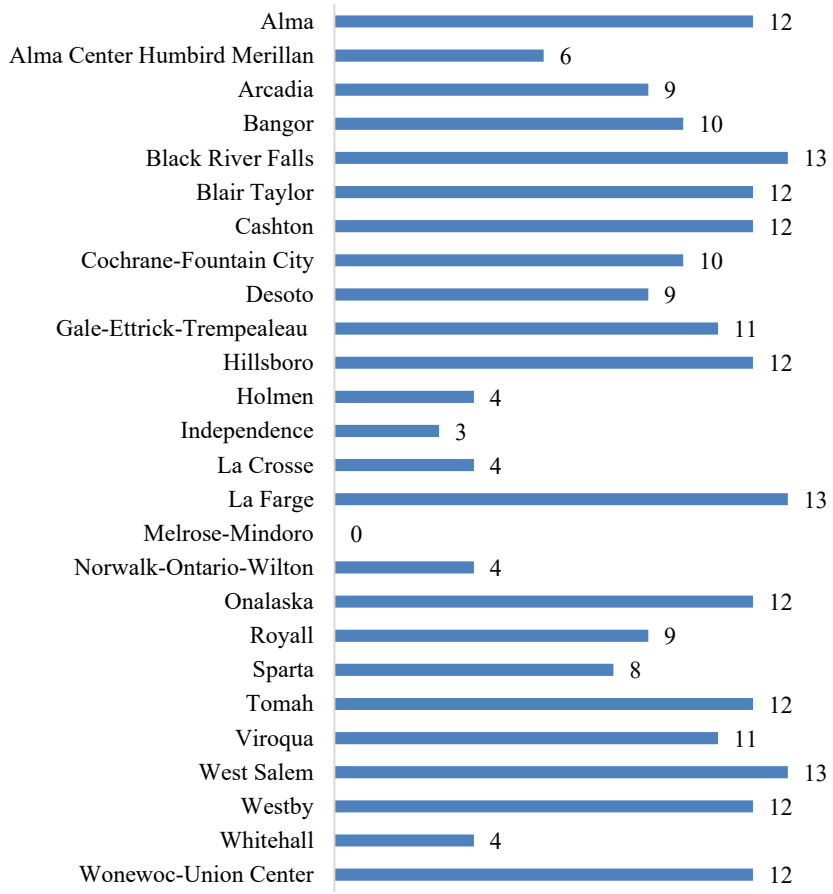
1. How is student data privacy protection addressed in the student records sections of school board policies in public school districts in CESA 4 in Wisconsin?
2. How do these local policies address federal student privacy obligations?
3. Who do these policies task with leading and managing the implementation of student data privacy policy?

The first section of this chapter is an overview of how these school districts address student data privacy through the policy documents collected for this study. The chapter's next portion describes how the policies' student records section address data privacy. The next section describes how the federal regulations for student information are addressed within the policies of these CESA 4 school districts. Finally, the last section of this chapter will disclose how the policies describe the responsibilities of school leaders for safeguarding and using student data.

Overview of Policy Approach to Student Data Privacy

Before addressing the first research question, this opening section will provide an overview of the types of policy documents collected for this study. To understand the three research questions for this study, I gathered 237 relevant policy documents from the 26 districts within CESA 4 (Figure 2). The school district of Melrose-Mindoro did not provide policies after multiple email requests.

Figure 3 - Collected Student Data Policy Documents



Wisconsin has no mandated approach to district policy organization, so there is variance with how the districts store, index, and make policies available to the public. Generally, the policy books are organized according to the function of the policy within the district. Some of these categories include policies for programs, students, staff, and operations. Within each of

these broader categories, dozens of separate policy sections are labeled with a distinct policy number and title. As an example of this organization, the student acceptable use policy for Onalaska schools is number 7540.03. It is one of 31 separate policy sections within the 7000 series for procedures regarding district property. Each district policy book contains dozens of separate policy segments, each with a distinct title and policy number, which I will refer to as *sections* or *documents* throughout chapters 4 and 5.

My collection process consisted of an initial review of the online policy sections labeled as *student records*. In this initial review, I noted references to other policy sections within the same district and downloaded those. I created a table within a research memo to record which policy sections I found within each policy book and then used this table to assist in finding comparable documents among all the districts. It was easy for districts using the same policy indexing system to locate the same sections because they typically had the same policy section numbers. For districts using a different organization method for their policies, I would search the policy titles and find those like the sections found in the initial search.

Policy Organization Methods

One way to understand the approach to maintaining student data among these district policies was to examine their organization and hosting methods (Table 5). Most districts use the hosting platform BoardDocs for storing, searching, and making their policies available to stakeholders. BoardDocs is a paid service provided to districts by Neola, an educational consulting firm specializing in board policies (Neola, 2022). The Neola service provides policy templates to ensure compliance with federal and state regulations and to address specific local district needs. While Neola provides its policy consulting service in multiple states, they utilize legal firms within each state to provide state-specific regulatory expertise. The Neola service

provides districts with biannual policy updates, which are then presented to their school districts for consideration of adoption by local school boards.

Table 5 - Board Policy Hosting Method by District

BoardDocs	Transitional BoardDocs	Local Hosting
Alma	Cochrane-Fountain City	Alma Center-Merillan-Humbird
Arcadia	La Crosse	Gale-Ettrick-Trempealeau
Bangor	Sparta	Holmen
Blair Taylor		Independence
Cashton		Melrose-Mindoro[a]
Desoto		Norwalk-Ontario-Wilton
Hillsboro		Whitehall
La Farge		
Onalaska		
Royall		
Tomah		
Viroqua		
West Salem		
Westby		
Wonewoc-Union Center		

[a]The Melrose-Mindoro district provided no policy documents for this study.

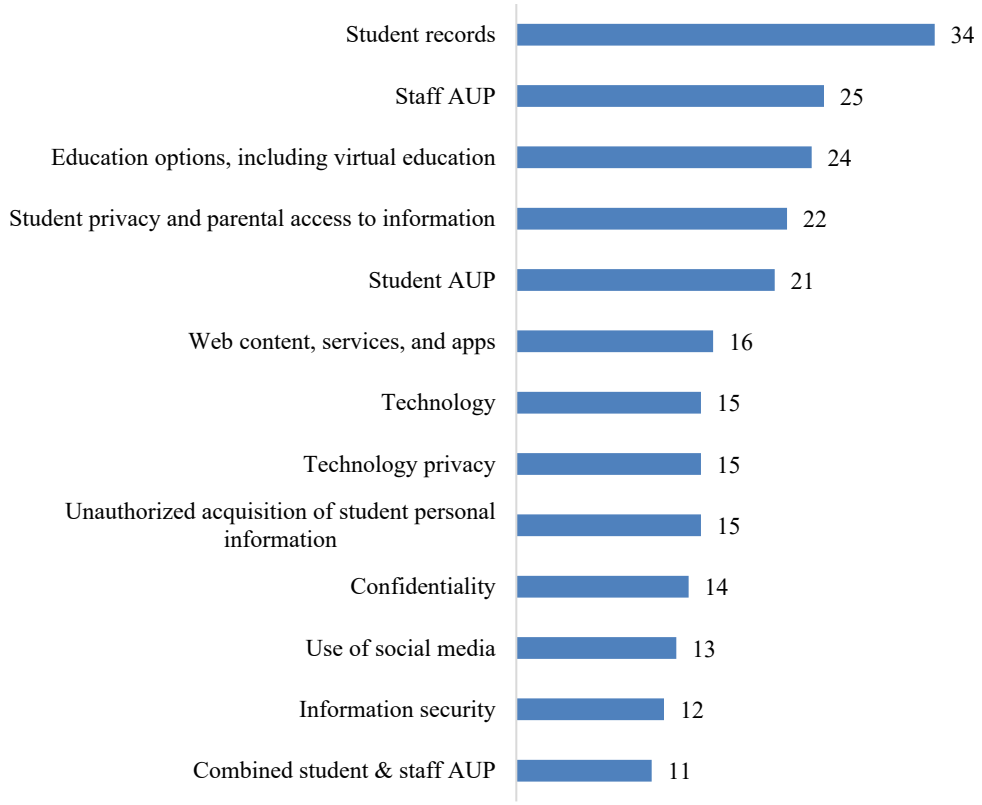
Three school districts in this study host their policies on the BoardDocs platform but do not use the policy templates from Neola. These districts are transitioning to using the full Neola policy process but host their current board policies in the BoardDocs platform. The other seven districts use various methods to store and make their policies available to stakeholders. These methods include Google Drive, hosting on the district web page, and local storage methods, which are not published. Still, the Wisconsin Open Records law makes the policies available upon request.

Relevant Student Data Policy Sections

Student data privacy guidelines were present within various policy sections from the 25 districts providing policies in this study. Figure 3 shows the number of policy documents collected according to the section in which they were found. While policy documents were

collected from 25 districts, some of them had multiple policy sections categorized according to the descriptors in Figure 3 below.

Figure 4 - Policy Sections Containing Guidelines for Student Data



Policy Section Descriptions

The following section will briefly describe the type of policy language found in each policy category from Figure 3 above and their relevance to this study.

Student Records. These policy sections commonly provided definitions of terms found within the FERPA regulation. These include the terms *education records, personally-identifiable information (PII)*, *directory data*, *legitimate interest*, *parent consent*, and *school officials*. The student records sections describe the procedures for transferring student records from one district to another, how districts disclose student information to court systems and law enforcement, and

how they share directory data with third parties without parental consent. Typically, student records sections also define directory data and the procedures for collecting and disclosing that type of student information. There were five policy documents categorized by the districts as *directory data*, but they have been included in the student records sections for this study. These five documents came from four districts and all use a local hosting and organization method.

Acceptable Use Policies (AUPs). Most school districts had separate policies for students and staff to guide their use of district technology resources, but some policy books used a combined AUP for students and staff. The policies for students typically note that technology is a crucial tool to support their education. For example, student policies would often address web filtering in compliance with the federal CIPA regulations and note that staff members would monitor student use of technology in addition to technical monitoring tools. Staff policies were similar, with language stating the value of technology in education, web filtering related to CIPA, and staff members' role in the appropriate safekeeping of student PII and other educational records.

Educational Options. These policies described the other approaches districts would use to provide appropriate educational services to their students. These alternatives included partnering with local higher education institutions, independent study programs, and summer school programming. Most relevant to this study, some of these policies described virtual education programs using third-party providers.

Student Privacy and Parental Access to Student Information. Generally, these policies described the rights of parents to inspect instructional material used with their children in the district. More relevant to this study, several policies also describe parent rights for

inspecting data collection instruments used in surveys given to students. Often these policy sections addressed parent rights provided through the federal PPRA regulations.

Confidentiality. Policies labeled with this title came from 14 districts using the Neola BoardDocs service, and they provide general statements about the importance of maintaining confidentiality with student information specifying that student records are exempt from the state law regarding public records. The three other district policy documents using local indexing methods contained similar language to those in their student records sections, describing the appropriate procedures for disclosing student records to parties outside the district.

Web Content, Services, and Apps. These policies provided guidelines for using these software technology resources and the expectations for their selection and approval by school administrators. These sections commonly described the appropriate use of these services with the privacy of student information as a requirement. In addition, policies in this category often outlined the expectation of these service providers to comply with federal regulations (FERPA, COPPA, CIPA) with student information.

Technology. The use of technology resources is addressed within the AUPs, but 14 of the BoardDocs districts and one local hosting district had brief policies I categorized as *technology*. These policies include statements about the value of technology as an educational tool but specify the appropriate use of these resources by students and staff as outlined by their AUPs. Most of the policies in this category also describe how school leaders would develop and participate in district technology planning.

Technology Privacy. These policy sections were all from the BoardDocs districts and primarily state that the district has the right to monitor and inspect staff members' use of district-owned technology resources. These documents don't directly address the appropriate care of

student information. Still, they are included in this study because they outline the responsibilities of the school leaders, and this concept is relevant to the third research question regarding leadership for implementing privacy policies.

Unauthorized Access of Student Information. These policy sections were only found in the BoardDocs districts and describe the district's response due to a breach of student PII. These districts also have corresponding policies for the breach of staff information, but I did not include those policies in this study.

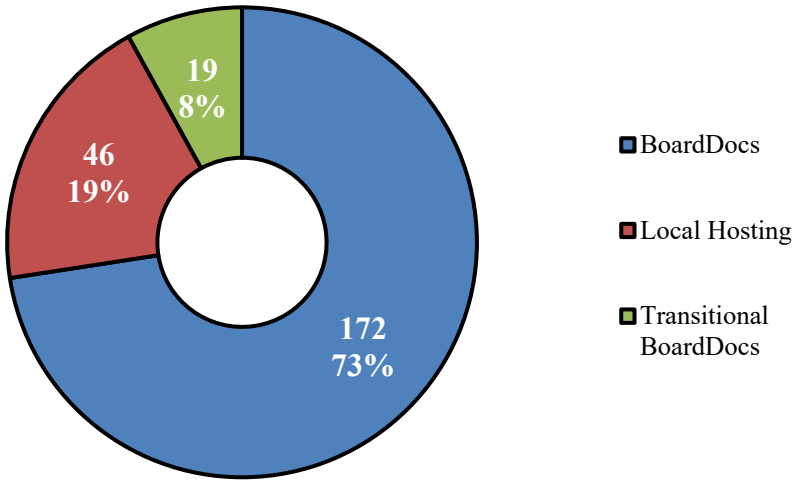
Use of Social Media. These policies outline students' and staff members' expected use of social media. Of relevance to this study are the portions from these policies which outline staff expectations for not disclosing student PII or doing so after receiving parental consent to share student PII on social media platforms.

Information Security. These policy sections contain descriptions of the expectations for third parties who utilize student data. These policies also describe the various responsibilities of school administrators for developing and enforcing plans with these third parties who the district has given student data.

Documents Collected by Policy Organization Method

As seen in the policy section descriptions above, most of the documents collected in this study are from districts using the Neola policy advising service (Figure 4). There is a similarity in the policy language but not uniformity among the 15 districts which use the Neola policy templates and updates. Local districts can change or decline the language found within the initial service templates and the periodic Neola updates. While the overall code application among the corresponding policy sections was similar among the BoardDocs districts, each section was examined to note differences and similarities in the expectations outlined in each document.

Figure 5 - Proportion of Collected Source Documents



Policy Sections by District

Table 6 further describes the source of the 237 documents collected for this study and the count of relevant documents accumulated from each district's policy books. While there are often hundreds of policy sections within a district's complete policy book, the sections that address student data were found within these 13 policy categories.

Table 6 - Number of Policy Documents by Section

	Staff AUP	Student AUP	Student records	Confidentiality	Unauthorized acquisition of student personal information	Student privacy and parental access to information	Education options (including virtual)	Information security	Student & staff AUP	Technology	Use of social media	Web content, services, and apps	Technology privacy	District total
Alma	1	1	1	1	1	1	1	1	0	1	1	1	1	12
Alma Center Humbird Merillan	1	0	2	0	0	1	1	0	1	0	0	0	0	6
Arcadia	1	1	1	1	1	1	1	0	0	0	0	1	1	9
Bangor	1	1	1	1	1	1	1	0	0	1	0	1	1	10
Black River Falls	1	1	4	0	0	1	1	2	2	0	0	1	0	13

Blair Taylor	1	1	1	1	1	1	1	1	0	1	1	1	1	12
Cashton	1	1	1	1	1	1	1	1	0	1	1	1	1	12
Cochrane-Fountain City	2	1	3	0	0	2	1	0	1	0	0	0	0	10
Desoto	1	1	1	0	1	1	1	0	0	1	0	1	1	9
Gale-Ettrick-Trempealeau	2	3	2	0	0	1	1	0	0	1	1	0	0	11
Hillsboro	1	1	1	1	1	2	1	0	0	1	1	1	1	12
Holmen	0	0	1	0	0	1	1	0	1	0	0	0	0	4
Independence	0	0	1	0	0	0	1	0	1	0	0	0	0	3
La Crosse	1	1	1	0	0	0	0	0	0	0	1	0	0	4
La Farge	1	1	1	1	1	1	1	1	1	1	1	1	1	13
Melrose-Mindoro	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Norwalk-Ontario-Wilton	1	0	2	0	0	0	1	0	0	0	0	0	0	4
Onalaska	1	1	1	1	1	1	2	0	0	1	1	1	1	12
Royall	1	0	1	1	1	1	0	1	0	1	1	0	1	9
Sparta	1	1	2	0	0	0	1	0	2	0	0	1	0	8
Tomah	1	1	1	1	1	1	1	1	0	1	1	1	1	12
Viroqua	1	1	1	1	1	1	1	1	0	1	0	1	1	11
West Salem	1	1	1	1	1	1	2	1	0	1	1	1	1	13
Westby	1	1	1	1	1	1	1	1	0	1	1	1	1	12
Whitehall	0	0	1	0	0	0	0	0	2	0	1	0	0	4
Wonewoc-Union Center	1	1	1	1	1	1	1	1	0	1	1	1	1	12

Student Records Policies

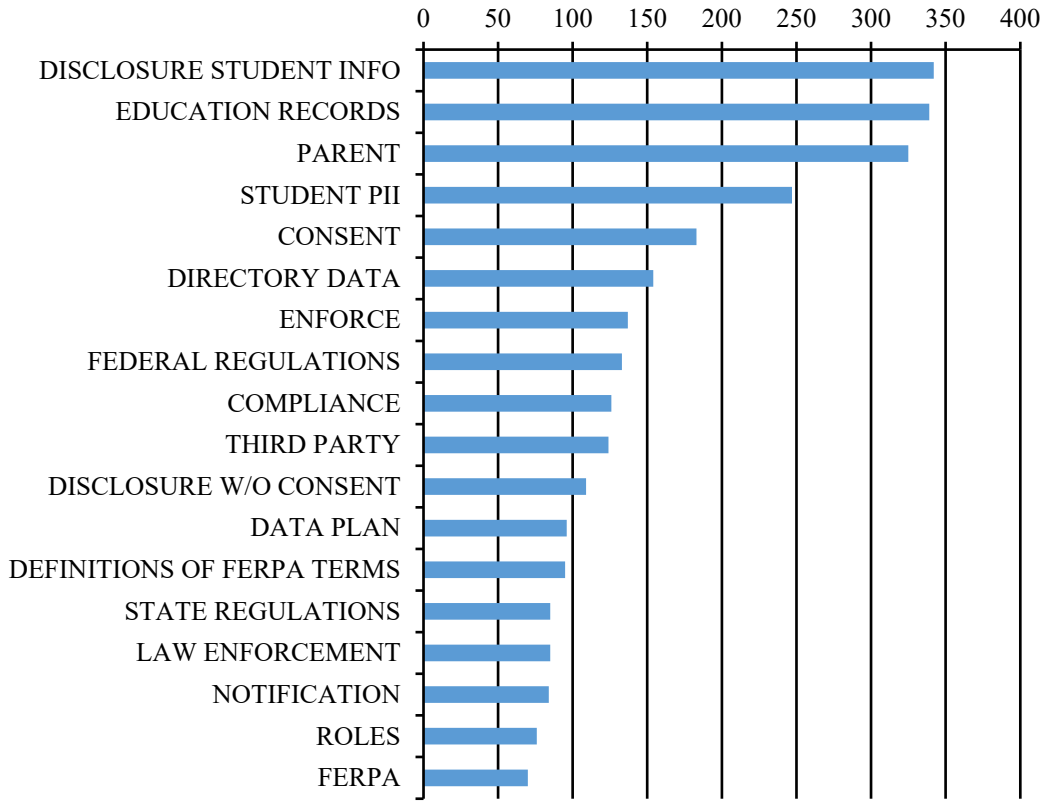
The first research question is based on the *student records* section of each policy book, and how these policies address student data privacy. The focus of the coding and examination for this question came from the policy documents labeled as *student records* by each district. I collected 34 policy documents from the 25 districts that provided policy media for this study. Table 7 shows the number of student records sections organized by host method.

Table 7 - Student Records Documents by Host Method

BoardDocs	15
Transitional BoardDocs	6
Local Method	13

In total, 61 different codes were applied 3954 times among 656 excerpts in the student records documents (Figure 5). To appropriately and consistently code all these documents, I used the search feature of Dedoose to find references for each term from the coding table. Then, I would find each specific occurrence of that term or concept and tag the word or phrase with the code. I repeated this process for each document categorized as a student record policy. Once all the codes were applied, I reread each document and then created larger coding excerpts based on the sections within the documents. I then applied the codes for these individual words and phrases to the larger excerpt in which they were found.

Figure 6 - Code Application Frequency of Student Records Policies



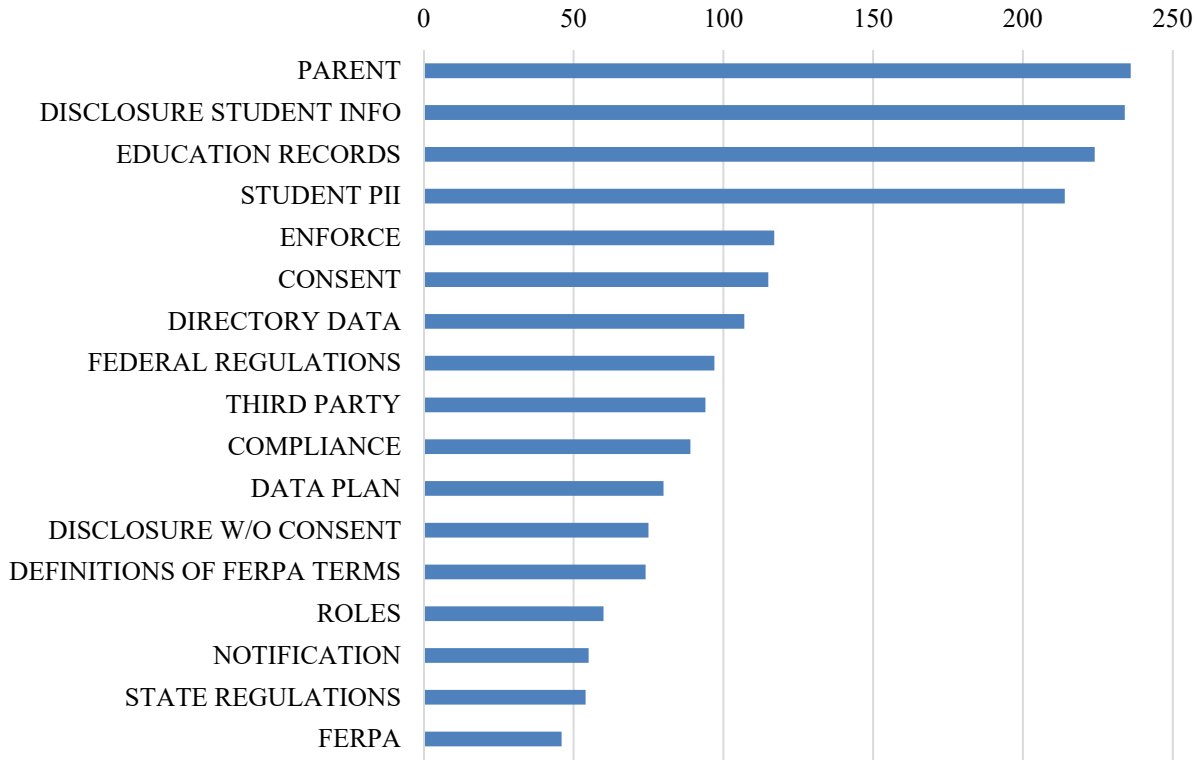
As the titling of these policy sections would imply, the coding application results show how districts will appropriately collect, maintain, and disclose the records of students. The most frequent code applications in these sections were for *disclosure of student information*, *parents*,

parent consent, *education records*, *student PII*, and definitions and procedures for student *directory data*.

BoardDocs Student Records Sections

For district policies using the BoardDocs hosting and policy service, 52 codes were applied 2824 times in 444 excerpts (Figure 6). Like the code frequency of all the student records, the most common code applications for the BoardDocs documents were disclosure of student information, parents, parent consent, education records, PII, directory information, and references to federal regulations.

Figure 7 - Code Application Frequency of BoardDocs Student Records Policies



Each student record section from the BoardDocs policies was titled *Student Records* with policy number 8330. These BoardDocs student records sections describe general use and procedures for collecting, storing, maintaining, and disclosing student information.

Use of Student Information Statements

All 15 of these policy sections started with a statement about the necessity to use and safeguard student information. An example of this statement from the Viroqua school district states:

> In order to provide appropriate educational services and programming, the Board must collect, retain, and use information about individual students. Simultaneously, the Board recognizes the need to safeguard students' privacy and restrict access to students' personally identifiable information.

There are minor variations of the wording of these statements among the 15 districts, but largely they are identical.

FERPA Definitions

These policies define key terms from the FERPA regulations, including *education records*, *directory data*, *student personally-identifiable information*, *parents*, *school officials*, and *legitimate interest*. In addition to the general definition of these terms, these policies give examples of the data types. Directory data includes the student's name, their participation in sports and activities, height and weight if used for sports documents, graduation date, and awards the students may have received.

The PII definitions in these sections provide examples, including the student name, parent names, address, personal identification numbers, and "other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school communication, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty." This definition and PII examples are similar to the definition provided by the U.S. Department of Education (2022a).

The definition for *school officials* within these policies states they are "a person employed by the Board as an administrator, supervisor, teacher/instructor, or support staff member." They can also be Board members, people contracted to perform a service for the district, parents on official committees, or volunteers sanctioned by the district. This policy language is also in line with the definitions and examples provided by the US DOE (2022b). These policies define *legitimate interest* as "direct or delegated responsibility for helping the student achieve one (1) or more of the educational goals of the District."

Disclosure Procedures

These BoardDocs student records policies outline the steps required to transfer student records to another school district, including the timeliness of disclosing the records, and procedures for gaining parent consent. These 15 policy documents also describe the requirements for sharing student information with law enforcement, social workers, and the court system. These policies also state that student PII may be shared without parents' consent in emergencies.

All 15 of these BoardDocs districts use similar language to describe the rights of parents to inspect survey instruments that collect students' personal information. These sections state that parents must make a written request to the building principal before the survey activity, and the principal will make the survey tool available to the parents. Another common portion of all these policies is that districts can release directory data information to college and military recruiters without the parent's written consent. Each of these districts uses the same language regarding recruiters. The policies specify that representatives of these organizations will sign a form stating that they will use the student information only to inform students of their services and that they will not release information to anyone beyond their recruitment team.

Third-Party Student Data Agreements

Each of these BoardDocs student records sections states the procedures for using student data when the district participates in a federal or state-sponsored audit or program evaluation performed by a third party. All 15 of the BoardDocs student records sections state that an agreement should be established with the entity to ensure they comply with the FERPA requirements. Three of the policies simply state that the district will enter into an agreement about using student data with the organization conducting the study or evaluation. The other 12 districts provide more detail about what this agreement will include:

> This written agreement must include 1) specification of the purpose, scope, duration of the study, and the information to be disclosed; 2) a statement requiring the organization to use the personally identifiable information only to meet the purpose of the study; 3) a statement requiring the organization to prohibit personal identification of parents and students by anyone other than a representative of the organization with legitimate interests; and 4) a requirement that the organization destroys all personally identifiable information when it is no longer needed for the study, along with a specific time period in which the information must be destroyed.

The statement above is specific to student data expectations for district participation in audits and evaluations. Still, there is another section found at the end of the policy books of 14 of the 15 (not found in the Arcadia student records policy) districts using BoardDocs. This statement appears to be more open-ended and inclusive of a variety of contexts when a district would share student information. That statement reads:

> Any entity receiving personally identifiable information pursuant to a study, audit, evaluation or enforcement/compliance activity must comply with all FERPA regulations.

> Further, such an entity must enter into a written contract with the Board delineating its responsibilities in safeguarding the disclosed information. Specifically, the entity must demonstrate the existence of a sound data security plan or data stewardship program, and must also provide assurances that the personally identifiable information will not be disclosed without prior authorization from the Board. Further, the entity conducting the study, audit, evaluation or enforcement/compliance activity is required to destroy the disclosed information once it is no longer needed or when the timeframe for the activity has ended, as specified in its written agreement with the Board.

This statement includes several expectations previously mentioned in the student records policies but clarifies what is required from these outside entities using student data from the district.

References to Federal and State Regulations

Each of these policy sections specifically mentioned the FERPA regulations for using student information within the policy body. Another federal regulation cited in the legal reference section of these policies was 20 U.S.C. 7908, which requires districts to provide directory data of students to military recruiters when requested. These policy sections also included references to Wisconsin statute 118.125, the state statute section which regulates how public school districts disclose student records.

Transitional BoardDocs Student Records Sections

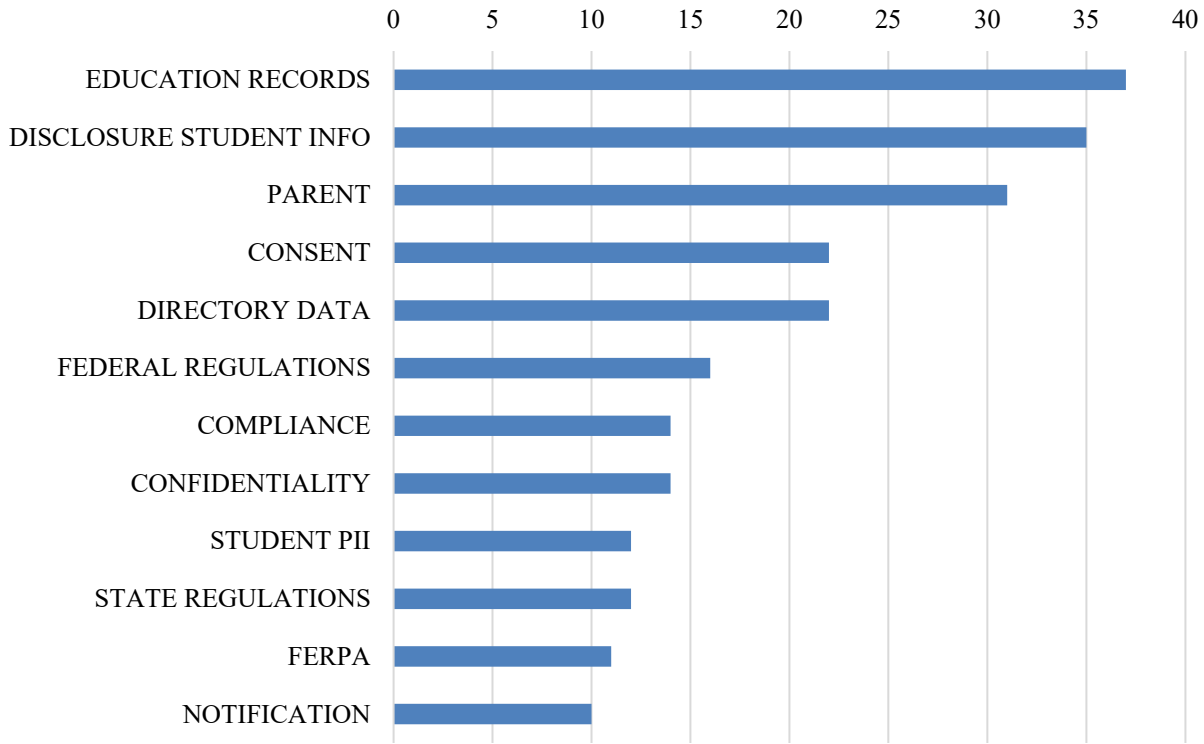
Three school districts are in the transitional phase of using the BoardDocs service. This means that they are hosting their board policies on the online platform but have not yet adopted the policy templates provided by Neola. From these three districts, there were seven total student records policy sections (Table 8).

Table 8 - Student Records Documents from Transitional BoardDocs Districts

District Name	Student Records Policy Documents
Cochrane Fountain City	3
La Crosse	1
Sparta	2

For the policies from districts in the transitional phase to using the BoardDocs hosting and policy service, 46 different codes were applied 371 times in 72 different excerpts (Figure 7). Like the code frequency of all the student records, the most common code applications for the transitional BoardDocs documents were education records, disclosure of student information, parents, parental consent, student PII, general references to confidentiality, and references to federal and state regulations.

Figure 8 - Code Frequency of Transitional BoardDocs Student Records Policies



These policy sections were titled student, pupil, or directory records, and the policy numbering system differed among the three districts. Like the BoardDocs districts, these transitional district student records sections describe general use and procedures for collecting, storing, maintaining, and disclosing student information.

Confidentiality Statements

The BoardDocs policies described in the previous section provide statements about the importance of using student data to be balanced by appropriately safeguarding this information. However, the language found within the transitional BoardDocs districts is focused on the confidentiality and security of student data and compliance with state and federal regulations.

The Cochrane Fountain City policy starts with, "The School Board recognizes the need for and importance of appropriately maintaining the confidentiality of individually-identifiable student records throughout the record life cycle." Similarly, the school district of Sparta states within their student records section, "Pupil records of any types and those not mentioned in this policy shall remain confidential and may be released only upon the receipt of written permission from the parent, guardian, or adult pupil."

The La Crosse student records policy provides the following expectation regarding student information used within the district:

> The School District of La Crosse believes that information regarding individual students must be treated in a confidential manner. Employees and volunteers working in the schools are expected to treat personally identifiable information about a student, such as, but not limited to, test scores, behavior, family background, health, and achievement, in a confidential manner. Thus, all pupil records maintained by a public school shall be

confidential, and will not be disclosed except as permitted herein or with the written consent of the parent or the adult student.

FERPA Definitions

All three of the districts provide definitions for *education records* and *directory data*. The examples of directory data among these three districts include student names, addresses, dates of birth, and student information relevant to extra-curricular activities. The La Crosse and Sparta school districts also provide specific examples of using directory data within the district or by district-affiliated third parties. These examples include local parent-teacher organizations, graduation vendors, yearbook vendors, playbills, honor roll publications, and athletic programs.

The Sparta and Cochrane Fountain City districts refer to student PII within their policies but do not provide definitions or examples. The La Crosse policy states that student PII includes test scores, achievement information, behavior records, family information, and health information. The La Crosse district provides a definition for *parents* as "biological parent, an adoptive parent, legal guardian, guardian ad litem, or a parent as defined under special education laws." The other two district policies do not define parents, but each specifies parents' rights multiple times within their student records policies.

The Sparta and Cochrane Fountain City policies provide definitions for *school officials* and *legitimate interest,* and those definitions are similar to what is provided by FERPA guidance from the USDOE (2022b). The La Crosse policy mentions the concept of legitimate interest within its student records policy but does not define the term.

Disclosure Procedures

All three of these districts describe the procedures for transferring student records to another school district and the requirement for documenting parent consent as part of this

information sharing. All these policies mention the procedures for providing student information to law enforcement agencies and personnel. The CFC and La Crosse districts provide statements about sharing student PII without parental consent in cases of emergency. While the BoardDocs policies mentioned the rights of parents to inspect data collection tools, none of these policies for the transitional districts included such language in their student records sections.

All the transitional districts state they will provide student directory information to military and college recruiters without parental consent. These policies do not mention a data agreement plan with recruiters, but they state that parents can opt out of information sharing to these recruiters.

Third-Party Student Data Agreements

Of the three transitional BoardDocs districts, La Crosse is the only one which provides policy language describing an agreement with third parties that recieve student information. That policy reads:

> The District will make available the Students' directory data and other student and pupil records to certain independent contractors and vendors, including, but not limited to, bus companies, assessment services, and database reporting services, who have been determined by the school board to have legitimate educational interests, including safety interests, in the records. The District will enter into confidentiality agreements with such independent contractors and vendors before sharing any student or pupil records to ensure that the records are only used in connection with the contracted services provided.

This statement states the district will enter into an agreement with these third-party entities but does not provide any additional information about what should be described in the agreement.

References to Federal and State Regulations

All three of these districts reference FERPA regulations within the body of the policy sections. La Crosse and CFC list Wisconsin's statute 118.125 in the legal references section of their policies. CFC also references Wisconsin statute 19.65, which defines the responsibilities of public officials, including school officials, for protecting private personal information. La Crosse and CFC also mention the Protection of Pupil Rights Amendments in their student records sections. While these three districts state they will provide student directory information to military and college recruiters, they do not list the legal reference, U.S.C. 7908, which requires this disclosure.

Locally Hosted Student Records Sections

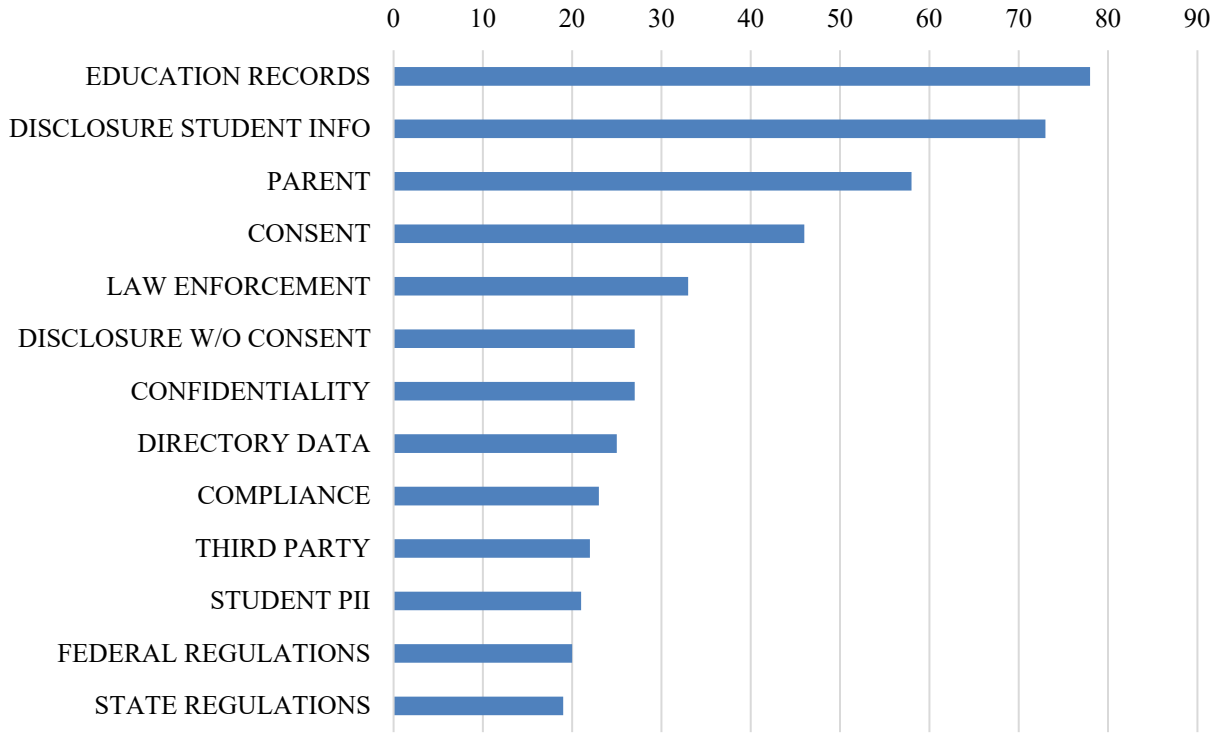
Seven school districts in this study do not use the BoardDocs service and host their board policies on their web page or another local service. From these six districts, ten total student records policy documents were collected and analyzed for this study (Table 9).

Table 9 - Student Records Documents, Locally Hosted

District Name	Student Records Policy Documents
Alma Center Merillan Humbird	2
Black River Falls	2
Galesville Ettrick Trempealeau	2
Holmen	1
Independence	1
Norwalk Ontario Wilton	2
Whitehall	1

From these district student records policies, 48 codes were applied 759 times in 143 excerpts (Figure 8). From these policy documents, the most common code applications were education records, disclosure of student information, parent, parental consent, law enforcement, disclosure without parent consent, directory data, and general references to confidentiality.

Figure 9 - Code Frequency of Locally Hosted Student Records Policies



Use of Student Information Statements

Among these district policies, five districts provide language in their student records policies stating the value of student information to support the education of the students. For example, the Holmen district provides this statement under the heading "Philosophical Statement," and it reads:

> Student records shall be maintained in the interest of the student to assist school personnel in providing appropriate educational experiences for each student in the district. The School District of Holmen maintains the confidentiality of personally identifiable information in the collection, storage, disclosure, and destruction. Persons collecting or using personally identifiable information are trained annually in confidentiality policies and procedures.

The Black River Falls, Whitehall, Galesville, and Alma Center districts have nearly identical statements in their policies, stating the importance of student information to provide appropriate educational experiences for their students, balanced by confidentiality with the student records.

The student records section from Norwalk does not contain a statement like the five districts above, but it emphasizes the importance of confidentiality with student records. The policy provided by the Independence district for this study is primarily about directory information. It has no Board statement about using student records for the students' educational experience.

FERPA Definitions

Four district student records policy documents describe what constitutes a student record. The Galesville, Alma Center, and Norwalk districts have nearly identical language for this definition. The Norwalk policy states:

> Student records include all records relating to an individual student other than notes or records maintained for personal use by teachers or other certified personnel which are not available to others, and records necessary for and available only to persons involved in the psychological treatment of a student.

The district policies also provide definitions and examples for specific types of student records, including progress, behavioral, law enforcement, court, and physical health records. The Black River Falls policy provides definitions for behavioral, physical health, and progress records. The student records policies from Independence, and Whitehall do not provide definitions of the FERPA concepts other than what constitutes directory data.

Like the policies of the districts using the BoardDocs service, the school district of Holmen provides an extensive list of definitions and examples of FERPA concepts. That policy

defines the different types of student records like the districts in the previous paragraph. The Holmen policy also defines the terms for parents, school officials, legitimate interest, and personally-identifiable information with language aligned with what is provided by the U.S. Department of Education (2022a, 2022b).

Disclosure Procedures

From these seven districts, the student records policies provided by Whitehall and Independence do not provide much detail for the guidelines for the disclosure of student information. The Whitehall student records policy is brief and only states the needs for confidentiality with student records, parental consent, and that student records can be "written, drawn, printed, spoken, visual, or electromagnetic information." The Independence policy document is about directory information with no guidance for disclosing other student information.

The policy documents from the other five districts provide guidelines for sharing student information when transferring to another school district and for sharing relevant information to law enforcement agencies and court systems. These policies also describe their processes for disclosing student directory data to military and college recruiters without parental consent. Still, there is no mention of a data use agreement in these situations. These policies also describe how they release student information in emergencies without parental consent.

Third-Party Student Data Agreements

Within the student records policies of these seven districts, only one statement pertains to using a data agreement when the district shares information with a third party. This statement comes from the Holmen district and is nearly identical to the one used by the La Crosse student records policy. The Holmen policy reads:

> The District will make available the Students' directory data and other student and student records to certain independent contractors and vendors, including, but not limited to, bus companies, assessment services, and database reporting services, who have been determined by the school board to have legitimate educational interests, including safety interests, in the records. The District will enter into confidentiality agreements with such independent contractors and vendors before sharing any student or student records to ensure that the records are only used in connection with the contracted services provided.

References to Federal and State Regulations

The student records section from the Independence and Whitehall districts do not reference FERPA. All districts except Independence list Wisconsin statute 118.125 in their student records policies. This is the state regulation guiding pupil records within Wisconsin public schools. Alma Center references state statute 19.65, the law requiring public officials to protect private information. While five district student records policies state they will provide directory information to military and college recruiters, Alma Center is the only district to provide the specific legal reference to U.S.C. 7908, which is the federal regulation requiring this disclosure.

Federal Student Data Privacy Regulations

The second research question for this study guided the examination of how school district policies address federal regulations for student data privacy. This section of the chapter begins with outlining the general presence of these regulations within the policy books. Then it moves into a closer examination of the Family Educational Rights Protection Act (FERPA), Protection of Pupil Rights Amendment (PPRA), and the Children's Online Privacy Protection Act (COPPA).

General Coding Presence

Specific references to these regulations were found within most of the policy books of the districts in this study (Table 10). However, the Melrose Mindoro district did not provide any of its policies after multiple requests, there were four documents from the Whitehall district, and the Independence district provided three documents.

Table 10 - Coded Federal Excerpts Presence by District

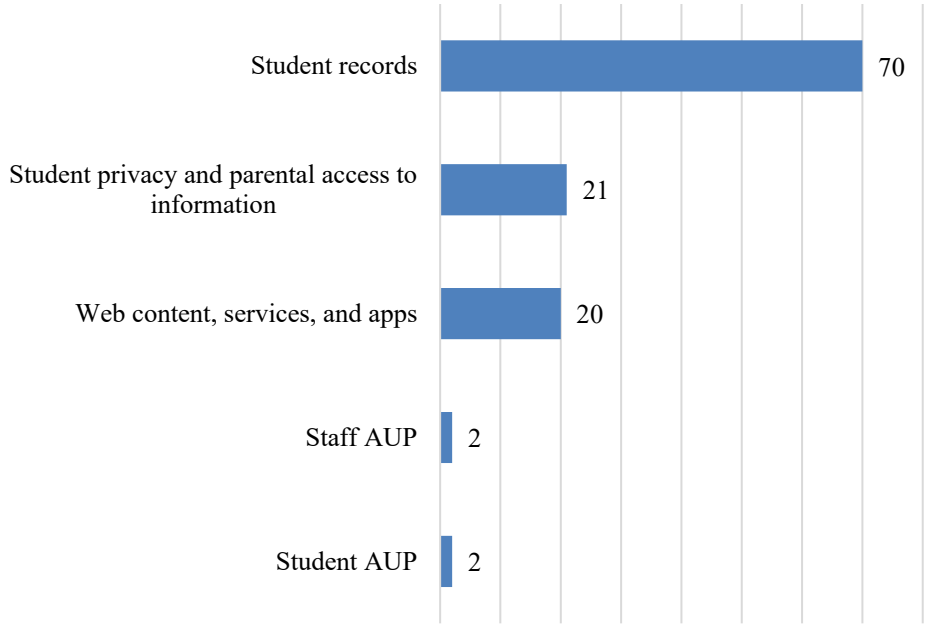
District	COPPA	FERPA	PPRA
Arcadia	1	3	1
Bangor	2	5	1
Blair Taylor	3	6	1
Alma	3	6	2
Alma Center Humbird Merillan	1	2	2
Black River Falls	0	3	4
Cashton	3	6	1
Cochrane-Fountain City	1	3	5
Desoto	2	5	1
Gale-Ettrick-Trempealeau	0	2	2
Hillsboro	3	7	1
Holmen	2	2	3
Independence	0	0	0
La Crosse	4	7	1
La Farge	3	7	2
Norwalk-Ontario-Wilton	0	5	0
Onalaska	2	5	2
Royall	0	5	2
Sparta	0	5	0
Tomah	3	7	2
Viroqua	3	7	2
West Salem	2	6	2
Westby	2	5	2
Whitehall	0	0	0
Wonewoc-Union Center	2	7	2
Totals	42	116	41

Family Educational Protection Act

FERPA was the most coded federal regulation among the three relevant to this study. The 114 specific references to FERPA were found in 61 different policy documents from 23 of the 25 districts with policies available for this research (Table 10 above). Approximately 60% of the FERPA references were found within the student records sections of the policy books (Figure 9). The federal regulation was also present in the policy sections for parent access to student

information, policies describing the technology services and applications used by the district, and acceptable use policies.

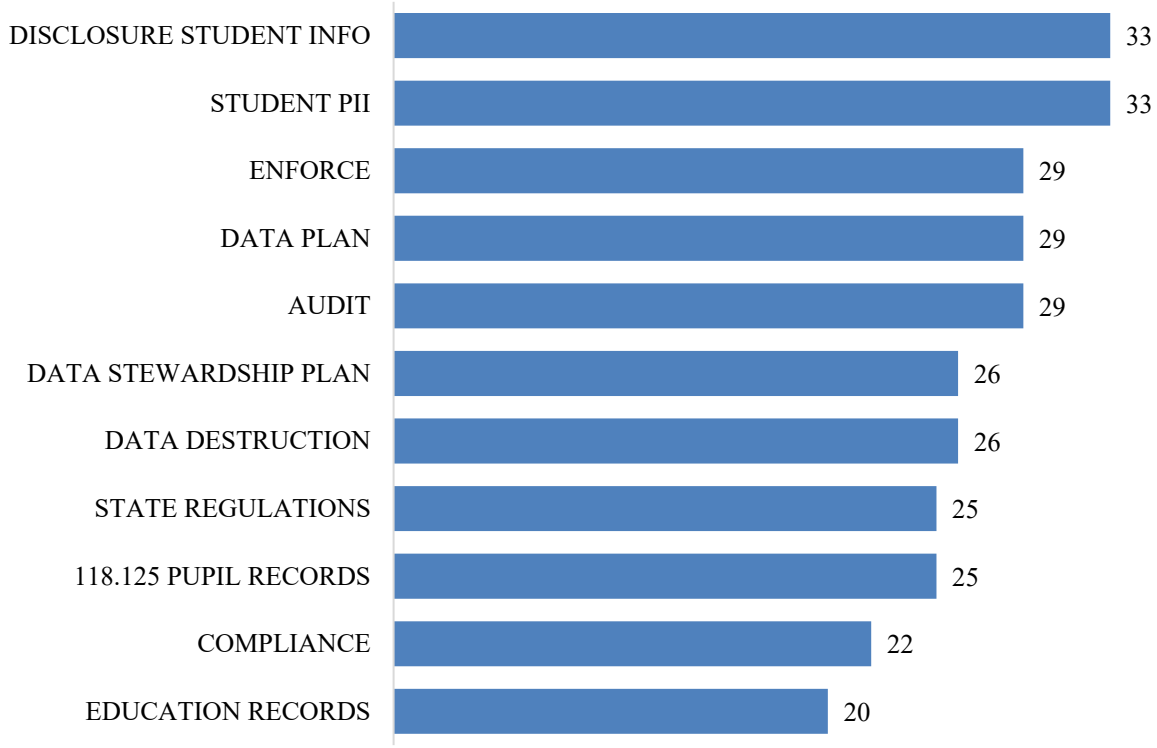
Figure 10 - FERPA Code Counts by Policy Section



Student Records Policies

FERPA was coded to 70 different excerpts within the student records policies. The section above for RQ1 provided a general description of the type of policy language found within the student records sections. The practical purpose of these sections is to provide procedural guidance for disclosing student information to various recipients. Another key purpose of the student records sections is to specify the rights of parents to control some of that disclosure and have access to the records of their children. Figure 10 shows the code co-occurrences with FERPA coding in these records sections to build on those findings.

Figure 11 - FERPA Coding Co-occurrences in Student Records Policies



The *disclosure of student information*, and *student PII*, are the most common co-occurrences with excerpts coded as *FERPA*. Disclosure of student information is the focus of these records sections and the purpose of the regulation itself. *Enforce* is another common co-occurrence for FERPA, and this code was used to mark passages of where the policies stated an expecation for the district or one of its employees to uphold a policy or the requirements from a federal or state regulation. The 29 co-occurrences of the codes *enforce* and *FERPA* all came from the student records sections of the districts using the BoardDocs service. More specifically, since these student records sections are similar, these co-occurrences came from two different sections of the policies. The first is the policy section which describes the expectation that a written agreement will be used when the district shares student information with an organization performing an audit or evaluation for the district. An example of the written agreement policy

language was previously shared in the *Third-Party Student Data Agreements* section for BoardDocs policies. In addition to this written agreement requirement, these policies also state:

> Under the audit exception, the District will use "reasonable methods" to verify that the authorized representative complies with FERPA regulations. Specifically, the District will verify, to the greatest extent practicable, that the personally identifiable information is used only for the audit, evaluation or enforcement of a government-supported educational program. The District will also ascertain the legitimacy of the audit or evaluation and will only disclose the specific records that the authorized representative needs. Further, the District will require the authorized representative to use the records only for the specified purpose and not to disclose the information any further, such as for another audit or evaluation. Finally, the District will verify that the information is destroyed when no longer needed for the audit, evaluation or compliance activity (Alma 8330).

This statement was used in 12 BoardDocs student records sections to show how the districts will ensure that parties using their student data comply with the FERPA regulation. Three districts use a less detailed version of this expectation: "The District will verify that the authorized representative complies with FERPA regulations."

Another common co-occurrence with the codes *FERPA* and *enforce* includes the *data stewardship* and *data destruction* tags. These occurrences are present in the statement at the end of these BoardDocs policies:

> Any entity receiving personally identifiable information pursuant to a study, audit, evaluation or enforcement/compliance activity must comply with all FERPA regulations. Further, such an entity must enter into a written contract with the Board delineating its

> responsibilities in safeguarding the disclosed information. Specifically, the entity must demonstrate the existence of a sound data security plan or data stewardship program, and must also provide assurances that the personally identifiable information will not be redisclosed without prior authorization from the Board. Further, the entity conducting the study, audit, evaluation or enforcement/compliance activity is required to destroy the disclosed information once it is no longer needed or when the timeframe for the activity has ended, as specified in its written agreement with the Board.

Student Privacy and Parental Rights Policies

There were 21 excerpts coded as *FERPA* within 15 policy documents categorized as student privacy and parental rights. These documents all come from policy 2416 from the districts using the BoardDocs service. The primary purpose of these policies is to guide the rights of students and parents regarding student participation in surveys that reveal specified types of sensitive information. These categories are specified within the PPRA regulation and will be explained later. The FERPA references in these policies are from the "audit and evaluation exception" of the regulation (USDOE, 2022). They are used to clarify the district's rights to disclose student personal information when it is collected for "the exclusive purpose of developing, evaluating, or providing educational products or services." In addition, these policies specify which evaluation activities can occur and do not require parental consent for student participation and student data collection. An example from Bangor policy 2416:

> tests and assessments used by elementary schools and secondary schools to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students (or to generate other statistically useful data for the purpose of securing such

tests and assessments) and the subsequent analysis and public release of the aggregate data from such tests and assessments.

Web Content, Services, and Apps Policies

There were 20 excerpts referring to FERPA from 12 different policy sections categorized for web content, services, and applications. All the policies came from districts using the BoardDocs publishing service. These policies describe the procedures used within districts when developing or choosing technology resources for educating students and communicating with the district's stakeholders. These policies reference FERPA in the sections that state how staff members are to gain approval for adopting technology resources. One example of this language comes from the Cashton school district:

> A teacher who elects to supplement and enhance student learning through the use of apps and/or services is responsible for verifying/certifying to the Director of Technology or Principal that the app and/or service has a FERPA-compliant privacy policy, and it complies with all requirements of the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA) and the ADA.

This type of language is present in 10 other *district web content, services, and apps* policies. Still, there is variance with which staff members verify compliance with FERPA and other regulations. The West Salem district does not have this language within its policy, but it does include FERPA in the legal references section.

Acceptable Use Policies

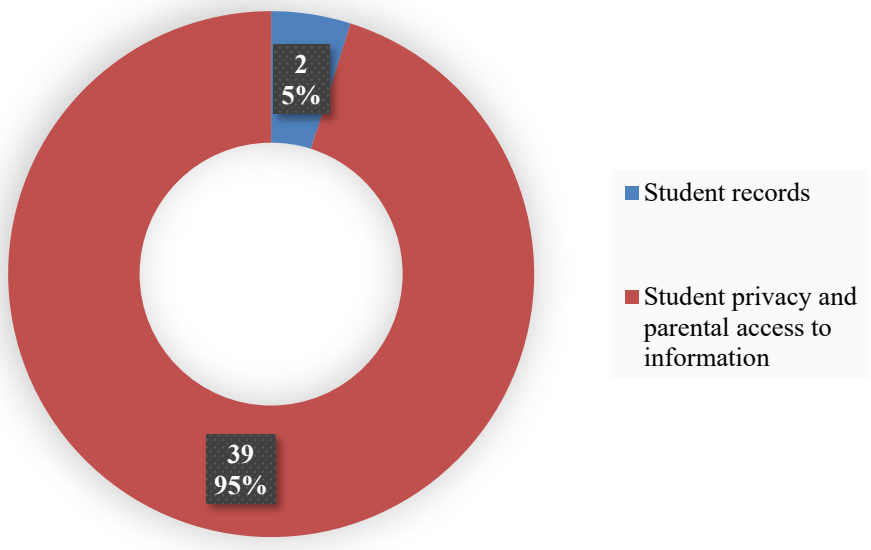
The four FERPA references came from two policies from the La Crosse district. Those policies are the staff AUP and the student AUP. Within the student AUP, the policy states, "Students will abide by personal privacy laws regarding digital information housed in district

systems and any online resources used as educational tools while a student in the district. Students can expect the district to follow the Family Educational Rights and Privacy Act." The staff AUP expectation is "Staff will comply with all state/federal laws or district guidelines/practices in ensuring confidentiality of student data including the Family Educational Rights and Privacy Act."

Protection of Pupil Rights Act

There were 41 specific references to the PPRA regulation in 23 different policy documents from 21 districts with policies available for this research (Figure 11). These references to PPRA were present in two different policy categories. Most of these references were from the policies categorized as *student privacy and parent access to information*, but there were also two references to PPRA found in *student records* policies.

Figure 12 - PPRA References by Policy Section



Student Privacy and Parental Rights Policies

The 39 references to PPRA in the student privacy policies were found within 21 documents from 20 districts. For the districts using the BoardDocs service, these policies all come from policy 2416, and their organization and content are similar. The beginning of these policies states that students are not required to participate without parental consent in a survey, analysis, or evaluation which reveals information in the following eight categories:

- political affiliations or beliefs of the student or his/her parents;
- mental or psychological problems of the student or his/her family;
- sex behavior or attitudes;
- illegal, anti-social, self-incriminating or demeaning behavior;
- critical appraisals of other individuals with whom respondents have close family relationships;
- legally recognized privileged and analogous relationships, such as those of lawyers, physicians, and ministers;
- religious practices, affiliations, or beliefs of the student or his/her parents; or
- income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such a program).

These eight categories come from the PPRA legislation (U.S. Department of Education, 2020b). The same eight categories are included in four districts using local policy hosting method and from the Cochrane Fountain City district in the transitional BoardDocs category (Table 11).

Table 11 - Districts Referencing PPRA 8 Categories by Host Method

BoardDocs	Transitional BoardDocs	Local Hosting
Alma	Cochrane Fountain	Alma Center
Arcadia	City	Black River Falls
Bangor		Galesville Ettrick Trempealeau
Blair Taylor		Holmen
Cashton		
Desoto		
Hillboro		
La Farge		
Onalaska		
Royall		
Tomah		
Viroqua		
West Salem		
Westby		
Wonewoc Union Center		

The PPRA regulation also requires districts to notify parents and students and allow them to opt out of participation if a survey requires collecting information from any of these eight categories. Parents and adult students also have the right to inspect the survey collection instrument. All 20 districts referencing PPRA in their student privacy and parental access policies address the notification, right to inspect, and right to opt out of participating in the survey. Here is an example from the Bangor policy book:

> Consistent with parental rights, the Board directs building and program administrators to: notify parents in writing of any surveys, analyses, or evaluations, which may reveal any of the information, as identified in A- H above, in a timely manner, and which allows interested parties to request an opportunity to inspect the survey, analysis, or evaluation; and the administrator to arrange for inspection prior to initiating the activity with students; allow the parents the option of excluding their student from the activity.

These policies also address the PPRA requirement to notify parents and students about surveys that involve collecting, disclosing, or using student information to market or sell the data. Alma Center is the only district among these 20 that does not explicitly address this PPRA issue within the student privacy and parental access policies. For example, the Onalaska 2416 policy says notice will be given for "activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or for selling that information (or otherwise providing that information to others for that purpose)." The other 19 districts have similar language to this example, all similar to what is explained in the PPRA regulation (U.S. Department of Education, 2020b).

Related, but not a requirement of PPRA, 14 of the 15 BoardDocs districts specifically state in these policy sections that student information will not be collected or disclosed for marketing purposes. For example, the Cashton policy states, "The Board shall not collect or use personal information obtained from students or their parents for the purpose of marketing or selling that information." However, the Onalaska district does not make this statement within this policy section. Instead, it states its position against collecting and using student data for marketing within the student records policy.

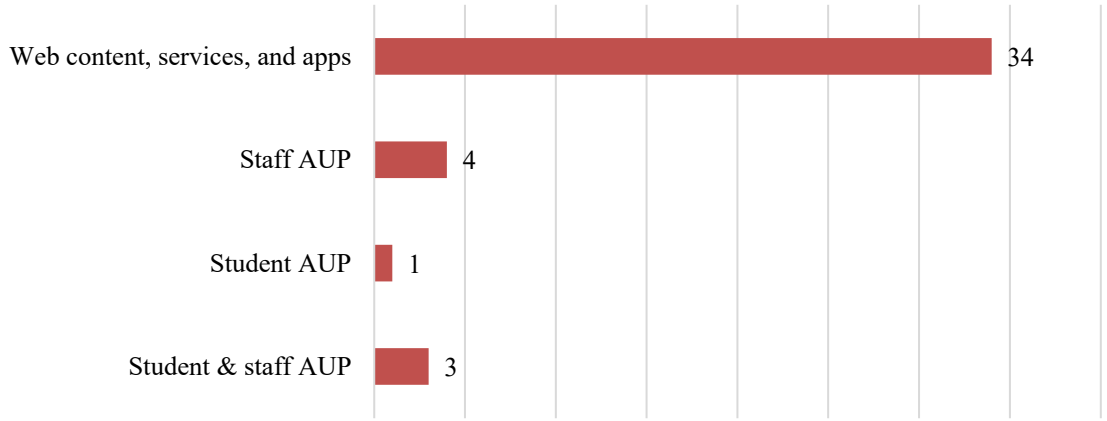
Student Records Policies

Two districts reference PPRA within their student records policies. The Cochrane Fountain City directory data policy lists PPRA within the legal references of that document, but the policy body does not contain PPRA language or related topics. The La Crosse district states that parents may contact the U.S. Department of Education for alleged non-compliance with FERPA or PPRA requirements. The La Crosse policy contains no other PPRA references or related topics.

Children's Online Privacy Protection Act

There were 42 references to COPPA in 19 different policy documents from 18 districts with policies available for this study (Figure 12). These COPPA references were found primarily within the policy documents for web content, apps, and services, but there were also references in staff and student acceptable use policies.

Figure 13 - COPPA References by Policy Section



Web Content, Services, and Apps Policies

All 34 COPPA references within this policy category came from 14 districts using the BoardDocs service, and their policies indexed as 7540.02. The Royall district uses the BoardDocs service but does not have a policy section for web content, services, and apps within their online policy book. Before examining these COPPA references, this next section will describe the guidance found within the two other policy books which address the use of web content, services, and apps.

Web Policies with No Federal References. Sparta and Black River Falls were the only two districts that have policies in this category but make no specific reference to COPPA within those policies. The Sparta web pages policy includes the statement, "To protect our students from the potential of danger, it is the policy of the Sparta Area School District to keep personal

information from our websites that would identify any individual student or provide information that would breach the privacy of an individual."

The Black River Falls policy is specific to web pages and does not mention other technology services like online programs and applications. Their policy describes the approval process for creating web pages and appropriate content. The policy lists the following expectations as student safeguards:

- Web page documents may include only information as designated by parents on the student's individual Acceptable Use Policy form.
- Documents may not include a student's email address, phone number, or address.
- Published e-mail addresses are restricted to staff members, community groups working with the district, or to a general group e-mail address where arriving e- mail is forwarded to a staff member.
- Decisions on publishing student pictures (video or still) and audio clips are based on the permissions given by parents through the Acceptable Use Policy form.
- Web page documents may not include any information, which indicates the physical location of a student at a given time, other than attendance at a particular school, or participation in activities.

This Black River Falls policy ends with:

> Given the rapid change in technology, some of the technical standards outlined in this policy may require change throughout the year. Such changes will be made by the District Technology Staff with the approval of the Superintendent. This Web Page Policy will be updated on an annual basis, or more frequently if required.

While the policy states the language may require more than annual updating, this policy was last revised in 2011.

COPPA References within BoardDocs Policies. These policies are based on a BoardDocs template. They all begin by stating that the purpose of technology resources used by the district is to educate, inform, and communicate. Resources should be appropriate for student use and be related to the curriculum. The policies state that technology resources may be used to communicate news about the district and to exchange information with stakeholders. The first COPPA reference found in all 14 policies is for pages created by district staff and students. That statement reads:

> All links included on the Board's website(s) or web services and apps must also meet the above criteria and comply with State and Federal law (e.g. copyright law, Children's Internet Protection Act, Section 504 of the Rehabilitation Act of 1973 (Section 504), Americans with Disabilities Act (ADA), and Children's Online Privacy Protection Act (COPPA)).

The reference to "above criteria" in this quote concerns the resources supporting education, information, and communication about the district's mission.

Eight district policies have a statement about web content, apps, and services created by a third party. That policy language states:

> Links included on the Board's website(s), services, and apps that pertain to its programs, benefits, and/or services must also meet the above criteria and comply with State and Federal law (e.g. copyright laws, CIPA, Section 504, ADA, and COPPA). While the District strives to provide access through its website to online content provided or developed by third parties (including vendors, video-sharing websites, and other sources

> of online content) that is in an accessible format, that is not always feasible. The District's administrators and staff, however, are aware of this requirement with respect to the selection of online content provided to students. The District's web accessibility coordinator or his/her designees will vet online content available on its website that is related to the District's programs, benefits, and/or services for compliance with this criteria for all new content placed on the District's website after adoption of this policy.

The staff member who serves as web accessibility coordinator varies among the districts.

Most of these policies have language which describes the process for approving the use of other applications and services beyond just content posted on web pages. For example, the West Salem policy states, "The Board authorizes the use of apps and services to supplement and enhance learning opportunities for students either in the classroom or for extended learning outside the classroom." The other 12 district policies follow this statement of support with what is required before a staff member will use the application or service. Here is an example of this from the La Farge district:

> A teacher who elects to supplement and enhance student learning through the use of apps and/or services is responsible for verifying/certifying to the Principal that the app and/or service has a FERPA-compliant privacy policy, and it complies with all requirements of the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA) and Section 504 and the ADA.

The staff member verifying the federal compliance varies among the districts and is seen in Table 12.

Table 12 - Federal Compliance Verifier for Instructional Apps and Services

District	Verifying Staff Member
Alma	Superintendent or Director of Technology
Bangor	Superintendent
Blair Taylor	Library Media Specialist
Cashton	Principal or Director of Technology
Desoto	Director of Technology
Hillsboro	Teacher
LaFarge	Principal
Onalaska	Superintendent
Tomah	Director of Technology
Viroqua	Director of Technology
Westby	Superintendent or Director of Technology
Wonewoc Union Center	Superintendent or Principal

Acceptable Use Policies

There were eight COPPA-coded excerpts from four school district policy books. Within the La Crosse staff AUP, staff members are asked to:

> Guide, teach, and model responsible use of digital devices and resources through current digital citizenship standards/guidelines, including monitoring students while they are using district digital resources in compliance with all laws including Children's Internet Protection Act (CIPA), Neighborhood Children's Internet Protection Act (NCIPA); Child Online Protection Act.

Additionally, the La Crosse staff AUP states that staff members may use online and social networking sites for educational purposes and to communicate with students, their parents, and other community members. This policy allows staff members to have their students create accounts with online services with the following guidance:

> District staff may allow students to create 'accounts' approved by the district for district devices that are necessary for using 'cloud' services, accessing resources, sharing information, turning in assignments, or communicating with teachers (for example).

> These accounts will be created in full compliance with COPA laws (all terms of agreements, including under age 13 restrictions, will be followed). District domains of any approved resources allows for the use by all district students. If a staff member wishes to have students under the age of 13 access online resources not approved by the district procedures that are restricted by age, then procedures to allow parents to set up the accounts with students will be used.

The age of 13 requirements are from the COPPA regulation, which stipulates that businesses cannot use the information from children under the age of 13 without their parent's consent (Herold, 2017). The Holmen AUP uses this same language to describe expectations for staff members who use technology resources with their students. The Alma Center staff AUP lists COPPA within its legal references section and states that the Director of Technology will "Address and prohibit the unauthorized collection, disclosure, and dissemination of personal and personally-identifiable information regarding students and minors, as particulary applicable to technology based resources."

The La Crosse student AUP lists COPPA in the legal reference section of the policy. Within the policy body, there is no specific mention of the regulation, but it is generally stated, "Students will abide by personal privacy laws regarding digital information housed in district systems and any online resources used as educational tools while a student in the district." Like the COPPA reference in the La Crosse staff AUP, this statement is found in the student AUP, "Students may be allowed to create 'accounts' in online resources approved by the district that are necessary for using 'cloud' services, accessing resources, sharing information, turning in assignments, or communicating with teachers (for example)." The Cochrane Fountain City student AUP lists COPPA, among other state and federal regulations, in the legal reference

section of the policy. No section of this AUP has content directly related to the COPPA regulation, but the appropriate and legal use of district technology resources is frequently mentioned.

Leading Data Privacy Policy

The third research question for this study is "Who do these policies task with leading and managing the implementation of student data privacy policy?" To address this question, I searched for specific leadership titles within each policy document and tagged them according to that title. After the initial rounds of coding these terms, I read through each document again to see the context in which the leader was mentioned and their role with policies related to the student information. This section begins with an overview of the coding presence and then moves into an examination of the specific leadership roles and the responsibilities they have with various student data policies.

Overall Leadership Coding Presence

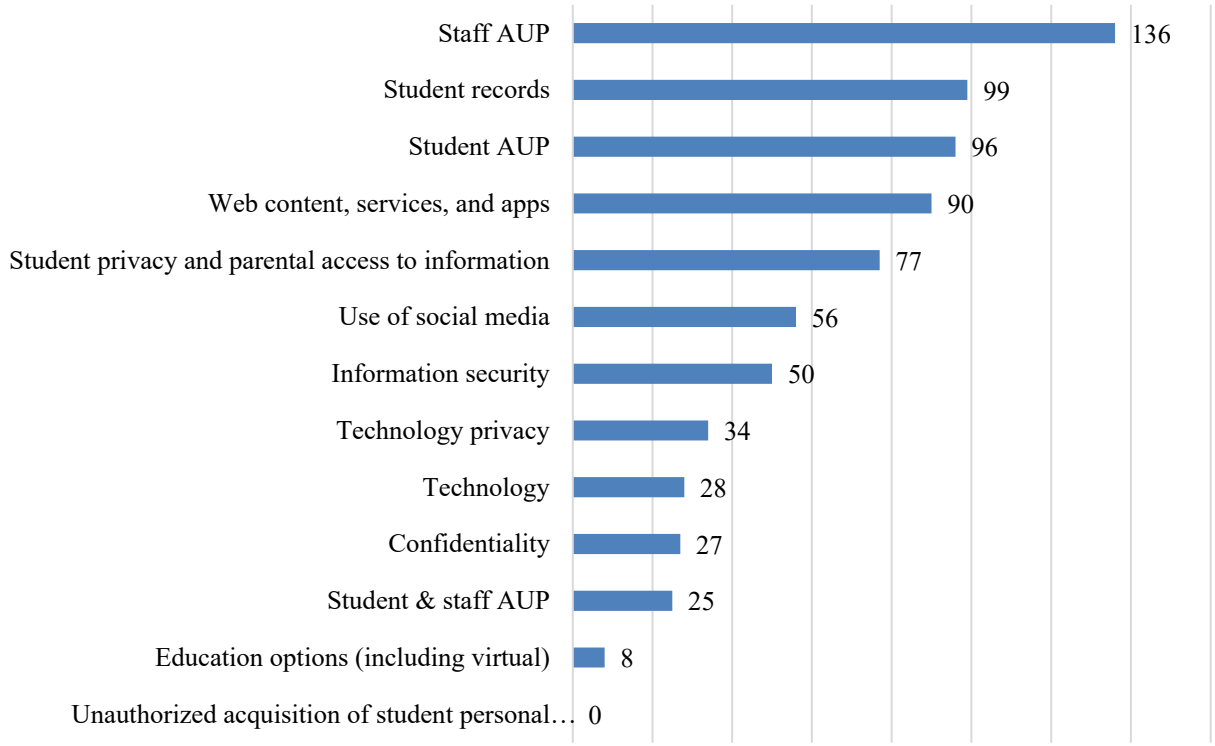
There were 558 policy excerpts which contained 726 relevant references to leadership roles for student data policies. These leader-coded excerpts came from 182 policy documents and from each of the 25 districts with policies available for this study. The roles of superintendent, principal, and director of technology were the three most referenced positions within the policies (Table 13) and will be the primary focus throughout the findings from Research Question 3.

Table 13 - Presence of Leadership Roles in Student Data Policies

Leadership Title	Number of Coded Excerpts	Number of Policy Sections Where Excerpted
Superintendent	373	156
Principal	227	137
Director of Technology	93	57
General reference to school leader	24	12
Web Accessibility Coordinator	19	7
504/ADA Coordinator	5	2
Public Relations Specialist	3	1
Library Media Specialist	3	1
Director of Business Services	3	2
Director of Human Resources	1	1

The referenced excerpts were found most often in the acceptable use policies and then the student records sections (Figure 13). In the policies for unauthorized acquisition of student personal information, there are no specific references to individual leadership roles, as all the references state "the district" instead of specific staff roles.

Figure 14 - Leadership References by Policy Section



Student Records

In the student records policies, there were 64 excerpts coded for superintendents and 33 for principals. There were no specific responsibilities outlined for directors of information within these policies.

Principal Responsibilities

Within the student records policies, seven of the districts (non-BoardDocs hosting) clearly state the principals' overall responsibility with student information with a statement like this from the Holmen district:

> The building principal, or his/her designee, shall have primary responsibility for maintaining the confidentiality of all student records kept at his/her school. All requests for inspection or for transfer of records should be directed to the building principal who

> will determine whether inspection or transfer is permitted. The building principal, or his/her qualified designee, shall be present to interpret behavioral records when inspection is made by the parent, their representative or by the adult student.

Principals are responsible for the records while at their school. They also determine whether someone may inspect records and should assist with explaining or interpreting some types of records when an inspection is allowed.

Another responsibility of the principals within three of these student records policies (Black River Falls, Independence, La Crosse) is to manage parent requests who want to opt out of the release of directory data. The Black River Falls also states that the principal is responsible for notifying parents of the directory data policy when families register in their school.

In the districts using the BoardDocs policy service, principals have only one specific responsibility within the student records policies. All 15 of these BoardDocs policies state that if parents want to inspect an instrument (survey) used to collect personal information from students, they are to contact the principal in writing before administering the data collection activity, and the principal will then make the instrument available to the parent.

Superintendent Responsibilities

The CFC student records policy makes the role of the superintendent clear with this statement:

> The District Administrator shall have primary responsibility for ensuring that District employees and other school officials who are authorized to create, collect, maintain, use, provide access to, or destroy student records understand their duties and responsibilities as defined by applicable law, Board policy, and District procedures (including the

specific confidentiality and maintenance requirements applicable to various categories of student records and other personally-identifiable records concerning students.

The superintendent needs to know the procedures and regulations for appropriately using student information. Still, they also need to ensure the rest of the district staff does. Later this policy states that the superintendent will provide the principal with "procedural and other technical assistance for the purpose of ensuring the confidentiality of all student records."

Seven of the districts not using the BoardDocs service specify that the superintendents are responsible for facilitating a hearing for records amendment if parents believe, "information contained in the student's records is inaccurate, misleading or otherwise in violation of the student's rights of privacy may request the District to amend the records (CFC 347 Rule)." This amendment process is a crucial aspect of FERPA (U.S. Department of Education [USDOE], 2022). Three of these policies also task the superintendent with creating an agreement with law enforcement agencies to share student information. The Whitehall policy makes no specific mention of the role of the superintendent, and the Independence policy notes that parents wanting to opt-out of directory data sharing will notify the superintendent.

There is consistency among the 15 policies using the full BoardDocs service. All these student records policies state the superintendent's responsibility for notifying parents annually about procedures for releasing directory data. These policies also task the district administrators with the notification to parents about the times when surveys and audits will occur that collect personal information from students. While there is consistency with these first two expectations from the BoardDocs policies, only eight of the policy books ask superintendents to prepare administrative guidelines to inform parents and students about their rights in the following areas:

- inspect and review the student's education records;

- request amendments if the parent believes the record is inaccurate, misleading, or violates the student's privacy rights;
- consent to disclosures of personally identifiable information contained in the student's education records, except to those disclosures allowed by the law;
- challenge Board noncompliance with a parent's request to amend the records through a hearing;
- file a complaint with the United States Department of Education;
- obtain a copy of the Board's policy and administrative guidelines on student records.

Another seven of these districts also ask their district administrators to develop procedural guidelines for:

- proper storage and retention of records, including a list of the type and location of records;
- informing Board employees of the Federal and State laws concerning student records.

Student Acceptable Use Policies

In the student AUPs, there were 92 excerpts that outline school leaders' responsibilities regarding student information (Table 14). These policies ask the superintendents to develop guidelines, lead the implementation, and share parts of these duties with principals and IT directors. Principals' primary responsibility is to train their staff members and ensure the students are educated about acceptable uses of technology resources.

Table 14 - Student AUP Leader References

Leader category	Number of References	Number of Policy Documents
Superintendent	45	14
Principal	30	16
Director of Information Technology	17	12

The non-BoardDocs student use policies did not contain language for the role of principals regarding student data privacy. The following findings are from the student AUP policy 7540.03 from the districts using the BoardDocs service. The policies begin with statements describing the value of technology as a learning and teaching resource. There are expectations for the legal and appropriate use of these resources. The district will use software to monitor student use and limit access to inappropriate content as defined by the Children's Internet Protection Act.

The primary responsibility of principals within these BoardDocs student AUPs is to provide training so that staff and students are knowledgeable about the policy. The policy states that students are to receive education about the following topics:

- safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
- the dangers inherent with the online disclosure of personally identifiable information;
- the consequences of unauthorized access (e.g., "hacking"), cyberbullying, and other unlawful or inappropriate activities by students online;
- unauthorized disclosure, use, and dissemination of personal information regarding minors.

These AUPs end with a statement about the responsibility for "initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District technology resources." All documents list the superintendent as having this responsibility shared with either the building principal (7 district policies) or the director of technology (7 district policies). Another responsibility of the superintendent is the oversight of

the configuration of the district filtering technology. This varies among the districts, but principals and technology directors share the responsibility to adjust the filter and block and unblock resources.

Staff Acceptable Use Policies

The relevant leader responsibilities in the staff AUPs are found primarily within the BoardDocs policies, but the staff AUP for Alma Center, with locally hosted policy methods, will be briefly described. This policy states that it is the responsibility of the director of technology to do all the following:

- ensure there is no access to inappropriate web content
- develop procedures for monitoring student use of technology
- develop an instructional program to educate students about appropriate and safe online behavior
- develop rules and procedures for safe and appropriate use for all other non-student users
- address and prohibit the unauthorized collection, disclosure, and use of student PII
- provide notice to all staff users of consequences for misuse of district technology resources

These responsibilities are significant and address a wide range of school operations. The district asks the director to manage the network components and provide procedural and curricular guidance to students and staff.

The BoardDocs staff acceptable use policies are like the responsibilities outlined in the student AUPs. Superintendents lead the overall guideline and procedure development and lead the enforcement of the staff AUP. Superintendents have oversight of the implementation of the district filtering and monitoring software, and the responsibility for filter adjustment is shared

with principals and the IT director. The responsibilities of the principals to provide training to their staff is clear, and the content of that training for the staff focuses on the four areas listed in the previous student AUP section. Like the student AUPs, the superintendents are responsible for initiating, implementing, and enforcing the staff AUPs with the principals and IT directors.

Table 15 - Staff AUP Leader References by Policy Host Method

	Superintendent	Principal	IT Director
BoardDocs	55	34	21
Transitional BoardDocs	5	5	1
Local Hosting	3	2	4

Information Security Policies

There are 10 policy books, all BoardDocs, with sections about information security. These policies provide classifications for confidential, controlled, or published data and the importance of following established security guidelines to use this information appropriately. The technology directors are listed as the point of contact for individuals who have questions about the security procedures. The policy specifies the responsibility of the superintendent to require training and define other procedures related to district data security (Table 16). There are no specific responsibilities assigned to principals in these information security policies.

Table 16 - Superintendent Responsibilities for Information Security Policies

Superintendents are asked to:

- Develop procedures in the event of an unauthorized release of breach[a] of information
- Require staff members to attend training for data security protocols
- Conduct periodic risk assessments related to security and access to district data

Note. These responsibilities are outlined in the BoardDocs Information Security policies.

[a]The Data Security policy 772 from Black River Falls, a locally hosted policy book, also specifies data breach responsibilities of the superintendent.

Confidentiality Policies

The purpose of these brief BoardDocs policies is to make clear the difference between confidential student records and other district documents which might be subject to disclosure under the state public records law. The policy says principals will grant or deny permission to staff members who want to remove education records from Board property. In addition, this policy directs the superintendent to "prepare guidelines concerning Board employees' duties to maintain certain information and records as confidential."

Technology Policies

These are all from BoardDocs policy books. Each of them begins with the statement, "The Board is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of District operations." Within nine of these policies, there are directives to the superintendent to develop and implement a District Technology Plan. These plan statements vary within each policy, but they include steps for resource evaluation, acquisition planning, and guiding staff and students for "safe, appropriate, and ethical use of district technology resources."

Web Content, Services, and Apps Policies

These policies set out the guidelines and approval process for the use of instructional technology within the district. Occurrences of leader responsibilities are in Table 17. Black River Falls (locally hosted) is the only district other than the BoardDocs districts to specify leader responsibilities within this policy category. Their policy describes the responsibilities of the superintendent and principals for approving the content of district web pages.

Table 17 - Leader References in Web Content and Services Policies

	Superintendent	Principal	IT Director
BoardDocs	30	4	13

Local Hosting	4	4	1
Transitional BoardDocs	0	0	0

The primary responsibilities for principals and IT directors within these BoardDocs policies are to ensure federal compliance of the apps and services used within their schools. Additionally, policies often name IT directors as the web accessibility coordinator within these policies. They ensure federal compliance with the content used or linked from the district web pages. The policies also task superintendents with this service and web content approval, in addition to leading the preparation of "administrative procedures defining the rules and standards applicable to the use of the Board's website and the creation of web content, apps, and services by staff and students." The Hillsboro school district also directs the superintendent to lead a periodic web content and services audit to ensure compliance with federal and state laws.

Conclusion

To understand the policy guidance for student data privacy within the school districts in Wisconsin's CESA4, 237 different policy documents from 25 districts were collected, coded, and analyzed. Examining each district's student records policies illuminated the policy guidance for collecting, maintaining, and disclosing education records and information deemed directory data. Results indicate that school districts using the BoardDocs policy service more commonly have language within the student records sections, which apply to contexts where student information is shared beyond the district. To understand how policies address federal student data protection regulations, the study focused on the FERPA, COPPA, and PPRA regulations within these policy books. Results demonstrate that the policies from the districts using the BoardDocs service had detailed language for satisfying the requirements of FERPA, COPPA, and PPRA. For the PPRA regulation, several non-BoardDocs policy books had detailed

guidance on meeting the requirements of the regulation. These policies were also examined to understand which district staff members are responsible for leading the policies addressing student data. Superintendents, principals, and IT directors were most often tasked with leading the work for student data privacy.

Chapter 5 provides further discussion of the findings of Chapter 4. The discussion will relate the current study to previous research and make connections to the study's conceptual framework. The next chapter will also present implications for practice and additional research.

CHAPTER 5: DISCUSSION AND IMPLICATIONS

In this study, I sought to understand how school board policies address student data use, especially regarding educational technology. American schools have increasingly adopted technology tools and resources to fulfill their obligations to students, staff, and communities. These tools are commonly used for instruction, day-to-day operations, stakeholder communication, and student data storage and analysis (Davies & West, 2014). After the passage of No Child Left Behind in 2001, school accountability movements required schools to participate in longitudinal data systems to gauge the effectiveness of districts, schools, and educators. During this transition period, many districts turned to third-party entities and vendors for support with the analytical and storage tools they possessed to handle large amounts of student data (Molnar & Boninger, 2015; Reidenberg et al., 2013). As schools began working with these third parties, parents, educators, and lawmakers expressed concerns about the security of student information, who had access to this data, and the privacy of the students (Bathon, 2013a).

The COVID-19 pandemic significantly impacted the increased use of technology, especially with virtual tools and resources. During this first phase of the pandemic, 77% of public schools reported moving at least some of their instruction to virtual platforms (Berger et al., 2022). The pandemic's impact on education continued into the 2020-2021 school year, as 62% of schools began the year in online formats (Roche, 2020). While educational technology allowed schools to continue during the pandemic, the concern regarding the privacy and security of student information remained.

During the initial shift to educational technology in the early 2000s and during the COVID-19 pandemic, school leaders looked to federal regulations for guidance with the growing

amount of student data. The Family and Educational Rights and Privacy Act (FERPA) was enacted in 1974 and was the initial regulation regarding the rights of students and parents and the use of student information. However, these tools' rapid technology utilization and growing capacities moved beyond the FERPA legislation. This caused concern about collecting, storing, disclosing, and using digital student information. Local districts and their leaders also looked to their district policies and state legislation to balance the beneficial use of the new technologies while still protecting the privacy of their students. The intersection of the nature of educational technology and the guidance from local and federal policies formed the basis of this study.

This study used the qualitative methodological approach of document analysis to examine student data privacy within school board policies as it relates to the use of educational technology. The policy documents came from 26 public school districts in one service agency area of Wisconsin. To understand the student data policies in this study, I followed these research questions to guide my inquiry.

1. How is student data privacy protection addressed in the student records sections of school board policies in public school districts in CESA 4 in Wisconsin?
2. How do these local policies address federal student privacy obligations?
3. Who do these policies task with leading and managing the implementation of student data privacy policy?

This study explored how these board policies address the federal regulatory requirements of student records and how boards addressed privacy in general through the privacy concept of *contextual integrity*, an established framework for exploring privacy and information flow (Nissenbaum, 2010). Additionally, this study examined school leaders' roles in implementing and managing student data privacy policies.

This chapter summarizes the findings from analyzing the board policy documents collected for this study. First, I review the contextual integrity framework and share the research themes and interpretations. I then discuss the implications for further research and practice and summarize the limitations of this study.

Summary of the Findings

The findings from the analysis of the policy documents were presented in Chapter 4, and a key theme was the differences in the Neola BoardDocs policies. There was more consistency among the BoardDocs policies since they come from the same original templates. Still, there were also noticeable differences in how student data privacy was addressed in those documents compared to the policies not using the Neola service. In the following section, I summarize the relevant findings organized by the research questions.

Student Records Policies

Most student records sections of all policy host types provide guidelines and procedures for the confidential treatment of student records. Generally, they define the primary terms found within the FERPA regulation. These include *education records*, *personally-identifiable information*, and *directory data*. These documents provide guidelines for transferring records from one district to another and for sharing student information with other entities like law enforcement, court systems, and military and college recruiters. These policies generally express parents' rights to consent to the transfer and parents' ability to inspect and amend records. These policies also address situations when the district can disclose student information without parental consent, like sharing information categorized as directory data. These types of information disclosure are not necessarily applicable to the current use of technology, which creates and disseminates student data.

An area of focus within the analysis of the records policies was to find sections that applied to situations where districts shared student data with third-party entities beyond the traditional types of disclosure described in the previous paragraph. The 15 student records policies using the BoardDocs service contain sections that specifically address the use of data by third-party entities to audit and evaluate programs to improve instruction. Each policy states the district will use a written agreement with the entity receiving and using the student data to ensure FERPA compliance. Of these 15 policies, 12 provide specific content in the written agreement. These agreements should define the specific purpose of the evaluation and the type of student information to be disclosed. The second component of the agreement is that the receiving entity will only use student PII for the specified purpose of the audit or evaluation. The next requirement for the agreement is that only members of the receiving entity with a legitimate interest in the contracted evaluation will use the student. The last component of the agreement is that the receiving organization will destroy the student data when no longer needed for its original purpose.

These BoardDocs policies provide another statement at the end of the student records policies, which applies to current uses of technology that rely upon the creation, collection, storage, disclosure, and analysis of student data. This section describes the responsibilities of the receiving entities and that they need to demonstrate the "existence of a sound data security plan or data stewardship program (West Salem 8330)." This written agreement must also state that the recipients will not redisclose the student PII without the district's permission. Like the agreement components in the previous paragraph, the third party receiving the student data must also agree to destroy the information at the end of the agreed-upon activity or service.

Two non-BoardDocs student records policies reference third parties' authorized use of data and specifically mention assessment and database reporting services. In addition, these policies state that confidentiality agreements will be used with the contractors to "ensure that the records are only used in connection with the contracted services provided (Holmen 347)." This language fits with modern technology uses of student information, but the policy requirements for the agreements are not as detailed as those from the BoardDocs policies.

Federal Student Data Privacy Regulations

The three federal regulations analyzed within these policy books were the Family Educational Protection Act (FERPA), Protection of Pupil Rights Act (PPRA), and the Children's Online Privacy Protection Act (COPPA). More than 60% of the references for FERPA were found within the education records policies, so the findings were like what was described in the previous section for student records policies. BoardDocs policies generally included specific definitions for key FERPA terms like *education records*, *parents*, *school officials*, *legitimate interest*, and *personally identifiable information*. Most policy sections referencing FERPA described the traditional practices for disclosing student records to other districts and local entities. The BoardDocs policies specifically mention the need for FERPA compliance when student data is used for audits and program evaluations by third parties contracted by the district.

An essential component of the PPRA legislation is the definition of the rights of parents and students when surveys and evaluations collect certain categories of sensitive information. These categories were included within all the BoardDocs policies and from five other policy books for a total of 20 policy sections. All 20 of these policies also include references to the rights of parents to be notified of surveys that may collect sensitive information. These policies also describe parents' rights to inspect the collection instrument and the right to opt the student

out of participating in the survey. Most (19) of these same policies also state they will notify parents about surveys that may collect and disclose student information for marketing. All 20 of these district policies describe the main components of the PPRA regulation. Still, only the policies from BoardDocs districts also require data agreements with the entities conducting the survey and using the student data.

References to COPPA were found in the policy books of 18 districts, and all but 4 of these districts were using the BoardDocs service. The primary concern of the COPPA regulation is to limit the ability of companies that operate websites and online services to collect and use PII from users under 13. The policies from the BoardDocs service specifically state that all technology resources used within the district must comply with the COPPA rule and other federal regulations. These policies also describe a process for approving instructional apps and services to ensure compliance with COPPA and other federal regulations. In addition, four policies from non-BoardDocs districts reference COPPA within the acceptable use policies.

Responsibilities of Leaders with Student Data Privacy

These board policies commonly task superintendents with creating guidelines and procedures for a variety of district functions. They develop the procedures and timelines to ensure they notify parents about their rights specified within federal regulations FERPA and PPRA. District administrators also outline procedures to account for the appropriate storage, disclosure, and retention schedule for student records and ensure district staff members are trained and able to follow these requirements and timelines for various types of student data. These policies also ask superintendents to create and enforce acceptable use policies for students and staff. Another aspect of the AUP responsibilities is to provide oversight for the implementation of web filtering and monitoring systems and delegate the day-to-day operations

of those tools to other administrators. Within the BoardDocs policies, superintendents are responsible for developing responses and communication plans in the event of a breach of confidential district information. The policies also ask superintendents to lead periodic risk assessments regarding data security and form technology planning groups to ensure technology resources' effective and appropriate use. District administrators act as facilitators when parents want to amend inaccurate student records or have concerns with the privacy of those records. Finally, district administrators are responsible for ensuring that the district and all its members comply with federal and state regulations regarding the protection of student information.

The primary responsibility of principals within these policies is to provide training to the school staff so they are knowledgeable about the safe and secure use of technology resources. In turn, the principals also ensure that the staff members can educate the students about their own safe and appropriate use of technology, with attention paid to the dangers of disclosing PII. The student records policies state that principals lead the work to properly store and disclose student records. Principals also provide notifications about directory data releases and work with parents who want to opt out of the releases. Principals are also responsible for allowing parents to inspect data collection instruments used with their students.

Both principals and directors of technology assist the superintendents with verifying apps and services used by staff members to ensure these resources comply with federal regulations. Both roles also support the superintendent with implementing and enforcing acceptable use policies for students and staff. Technology directors also work with the superintendent to change the district filtering and monitoring tools. In the BoardDocs policies, IT directors are listed as the point person for questions and needs that staff may have about information security processes.

Contextual Integrity

Nissenbaum's (2010) contextual integrity (CI) was selected as this study's conceptual framework to help explore privacy issues. As shown in Chapter 2, the overall scholarship for understanding privacy is lengthy and detailed. Rather than establishing a comprehensive conceptualization of privacy, contextual integrity focuses on the flow of information from one agent to another within a given context. The social systems in which the exchanges of information occur influence the expectations for how the data flows and to whom it flows.

Nissenbaum developed the CI framework during the dynamic growth of technology systems. These systems have an increased capacity to monitor and track information. Additionally, tools for aggregating and analyzing large amounts of information have dramatically changed in recent decades. Finally, the ability to distribute raw and analyzed data has become powerful and efficient. The CI framework recognizes the changing nature of technology and its influence on society. These technological advancements are undoubtedly present within school systems, and the framework is applicable to help understand the expected flow of information regarding student data.

The key CI terms to understand for this study are *contexts*, *norms*, *actors*, *attributes*, and *transmission principles*. The contexts are the situations in which information is shared or withheld. Within this study, the situations might be sharing student information with a state governmental agency for an audit or having students take an assessment from a third-party vendor for program evaluation purposes. The norms are the regulations that influence how or what information is shared. Board policies, local laws, and federal regulations are all norms. Actors are the people in the context who provide, share, and use student information. Attributes are the types of information shared. For example, student PII, behavioral records, and directory

data are attributes in this study. Finally, the transmission principles are the conditions in which information can or can not be shared. Parent consent, FERPA compliance, and data stewardship agreements are all examples of transmission principles for this study.

All these aspects within a context work together to determine integrity with how the information flows. Integrity is preserved when the actors follow the norms, and the appropriate information flows under the expected circumstances. These CI terms will be used to describe the guidelines within board policies and how the policy language outlines the appropriate and expected flow of student information.

Interpretation of the Findings

I believe this study has provided important information about how school districts attempt to balance the educational needs of their students, the effective use of technology resources, and then meet the privacy expectations of students and parents outlined by federal regulations. Expressed in these board policies are statements that show how districts value educational technology to support student learning. Also found within the policy books are statements valuing the need to protect the privacy of students and the confidentiality of student information.

My interpretations of the findings from this study are found within the following themes. The first is that using the contextual integrity framework is appropriate to understand the expected information flows of student information within these board policies. Another key finding is the need for district policies to describe obligations to follow federal regulations but state the procedures in a way that accounts for the modern uses of educational technology, which have powerful abilities to create, collect, analyze, and disseminate data about students. Finally, I believe that much is asked of school leaders to create, implement, and enforce procedures and

guidelines to ensure the appropriate use of student information while recognizing the growth of the capabilities of technology used in schools. Interwoven within these interpretations are the differences between the policies of the districts using the Neola BoardDocs services and those not using the service. Generally, the BoardDocs policies appear to provide more detailed descriptions of procedures and guidelines that address student data protection within systems that utilize current educational technology tools and services.

Student Records Policies

Wisconsin state legislation does not provide detailed guidance for the protection and privacy of student data. Therefore, the work of school leaders is to ensure that local board policies satisfy federal legislation regarding student data while still enabling the use of needed educational technology. The combination of these various federal regulations is challenging for leaders to track, understand, implement, and seek help for enforcement (Anderson, 2022; Electronic Privacy Information Center, 2022; Trainor, 2015; Venzke, 2022). With the lack of an all-encompassing federal or state law for the use and protection of student information, leaders are often faced with a patchwork of regulations and local expectations to meet the needs of district stakeholders (Strickland, 2019). Leaders must research best practices and applicable laws, and then work with their school boards to adopt local policies addressing the protection of student information. In Wisconsin, this policy creation and adoption process is left to the 421 individual districts, so there is variance in the policies and procedures for addressing student data practices within the districts.

This study has shown consistencies with these approaches for the districts using the same policy consultation service. Still, this research does not intend to state that one policy process is more effective. Instead, I will use the contextual integrity framework to explain how these

policies define expected flows of student information, focusing on the policies from the districts using the Neola service. To begin with, CI is based on the appropriate flow of information relative to the stakeholders of a social setting or context who have common goals and purposes (Nissenbaum, 2010). These contexts have social and informational norms about how information should flow.

Norms are stated throughout many of the policies in this study, but the focus here is on the 15 BoardDocs student records policies. These policies begin with the statement:

> In order to provide appropriate educational services and programming, the Board must collect, retain, and use information about individual students. Simultaneously, the Board recognizes the need to safeguard students' privacy and restrict access to students' personally identifiable information.

The expressed norm is that the district values a quality educational experience for the students, and using student data will help support the needed services and programs. The Board, composed of elected local community members, also values students' privacy and will protect their personal information.

Similar pro-technology norms are expressed in the staff and student acceptable use policies. For example, the student AUP begins with:

> Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning to incorporate the vast, diverse, and unique resources available through the Internet.

This norm statement recognizes the dynamic growth of technology used in society and education settings. This language from the AUP continues with:

> With respect to students, District Technology Resources afford them the opportunity to acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board provides students with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students.

Technology is valued within the educational setting, but the policy also recognizes that the skills learned within school are applicable and necessary outside and beyond the years the students are in the district.

These acceptable use policies also state how the district expects students and staff to follow formal legal norms:

> The Board regulates the use of District technology resources by principles consistent with applicable local, State, and Federal laws, the District's educational mission, and articulated expectations of student conduct as delineated in the Student Code of Conduct.

These examples of policy language do not provide detailed procedural direction. Still, they help one understand the type of educational experience provided to students and its connection to the use of technology.

Knowing the norms expressed in these policies show the value of technology, and we can look at examples of expected information flows within the student records policies. As highlighted before, these student records policies address the use of student data for participating in audits and evaluations, which help develop and improve district education programs. The policy allows administrators to disclose "personally identifiable information from education records, without consent, to organizations conducting studies 'for, or on behalf of' the District

for purposes of developing, validating or administering predictive tests, administering student aid programs, or improving instruction."

Applying the CI terminology, the conditions or *context* here is participation in an evaluation where the results provided needed information about district programs. The CI framework provides that *actors* can be *senders*, *receivers*, and *subjects* of the information. The sender, in this context, is the administrator providing student information. The *recipient* is the entity or organization receiving the student information, and the *subjects* of the information are the students. Another critical concept to understand is the *attribute* or type of transmitted information. This policy section states that the *attribute* is students' personally-identifiable information. The *transmission principles* within this policy statement are the conditions for sending the information. The principles here are that information can be sent, without parental consent, so long as the receiving entity is providing the specified service.

There is contextual integrity for the flow of information when the actors, transmission principles, and information attributes all follow the expected norms of the context. These board policies also serve as norms for information flow as they state the expectations for what information can be shared, by whom, to whom, and the context in which it can occur.

To understand how districts address student privacy in their policies, I examined other sections where the context involved sharing digital information from students (attributes) to technology-based third parties (recipients). The previous excerpt is followed in the student records policy with this section:

> Information disclosed under this exception must be protected so that students and parents cannot be personally identified by anyone other than a representative of the organization conducting the study, and must be destroyed when no longer needed for the study. In

order to release information under this provision, the District will enter into a written agreement with the recipient organization that specifies the purpose of the study.

There are several transmission principles or conditions of release found within this excerpt. First, the information must be protected and can not be viewed by members outside the intended receiving organization. Another principle is that the information is destroyed at the end of the activity or service. The last principle is that the district will not release information unless a written agreement is used. Establishing a written agreement is a principle for transmission, but the language within the agreement is considered a *context-relative informational norm*. This type of norm is more specific than the generalized organizational and social norms shared previously that show support for the use of technology.

These student records policies then provide a very detailed description of what the agreement (contextual information norms) will contain before student data is released to the third party. The agreements must include:

1) specification of the purpose, scope, duration of the study, and the information to be disclosed;
2) a statement requiring the organization to use the personally identifiable information only to meet the purpose of the study;
3) a statement requiring the organization to prohibit personal identification of parents and students by anyone other than a representative of the organization with legitimate interests;
4) a requirement that the organization destroys all personally identifiable information when it is no longer needed for the study, along with a specific time period in which the information must be destroyed.

The agreement has many transmission principles, including the destruction of student data and the disclosure limitation to additional recipients. This type of detail within a policy makes it clear what the expected flow of information will be and the conditions in which it will occur.

> One last portion of this policy section accompanies the previous two excerpts. It states: While the disclosure of personally identifiable information without consent is allowed under this exception, it is recommended that whenever possible the administration either release de-identified information or remove the students' names and social security identification numbers to reduce the risk of unauthorized disclosure of personally identifiable information.

In this excerpt, PII, de-identified data, student names, and social security numbers are all information attributes. These attributes are detailed descriptions of the data type involved in this information flow. The transmission principle allows for disclosure of these types of information, but the preferred principle is that information of this type is not disclosed.

These BoardDocs student records policies also state that the Board gives administrators the authority to:

> disclose personally identifiable information from education records without consent, to authorized representatives of the Federal government, as well as State and local educational authorities; The disclosed records must be used to audit or evaluate a Federal or State-supported education program, or to enforce or comply with Federal requirements related to those education programs. A written agreement between the parties is required under this exception.

The context here is an audit for a program compliance evaluation. The sender is the administrator from the district, the receiver is a member of the mentioned governmental entity, and the

information subjects are students. A written agreement is one transmission principle that specifies the conditions under which the student information will be shared.

The written agreement requirements for the use of student information in these governmental audits must include:

1) designation of the receiving entity as an authorized representative;
2) specification of the information to be disclosed;
3) specification that the purpose of the disclosure is to carry out an audit or evaluation of a government-supported educational program or to enforce or comply with the program's legal requirements;
4) a summary of the activity that includes a description of methodology and an explanation of why personally identifiable information is necessary to accomplish the activity;
5) a statement requiring the organization to destroy all personally identifiable information when it is no longer needed for the study, along with a specific time period in which the information must be destroyed;
6) a statement of policies and procedures that will protect personally identifiable information from further disclosure or unauthorized use.

This agreement description limits who the recipient can be with item 1 and specifies the information attribute in 2. Items 3 through 6 are all detailed descriptions of transmission principles to be satisfied before the student PII is shared with the entity.

The policy goes on to provide additional transmission principles. The recipients must comply with FERPA and the PII is only used for the specified audit. The district will only provide the specific records needed for the audit and states that the recipient will destroy the

student information after a specified time or after the audit. This policy is detailed and clearly expresses the expectations for how information can flow in this context.

Another relevant example of CI application is seen within the policy section describing how directory data will be shared with military and college recruiters without parental consent. The policy clarifies that the information attributes are the student's name, mailing address, email address, and phone number. The recipients are the recruiters; parental consent is not an expected transmission principle in this context. Additionally, the policy stipulates that the recruitment staff receiving the information sign an agreement stating they will only use the student directory data for their recruitment activities and not share the information beyond their organizations.

At the end of these BoardDocs student records policies, the final statement provides more detailed contextual integrity concepts for the district to share student data with a third party. That statement reads:

> Any entity receiving personally identifiable information pursuant to a study, audit, evaluation, or enforcement/compliance activity must comply with all FERPA regulations. Further, such an entity must enter into a written contract with the Board delineating its responsibilities in safeguarding the disclosed information. Specifically, the entity must demonstrate the existence of a sound data security plan or data stewardship program, and must also provide assurances that the personally identifiable information will not be redisclosed without prior authorization from the Board. Further, the entity conducting the study, audit, evaluation, or enforcement/compliance activity is required to destroy the disclosed information once it is no longer needed or when the timeframe for the activity has ended, as specified in its written agreement with the Board.

This language is detailed and specific in describing several transmission principles, and it allows for the flow of student PII within various possible contexts.

Aside from these BoardDocs student records policies, only Holmen and La Crosse school districts had language within their records policies relevant to digital student data used by third parties. These policies refer to independent contractors and vendors providing assessment and database services as potential data *recipients*. The *attributes* are only described generally as students' directory data and other student records. These two policies state that the *transmission principle* is for these recipients to have legitimate educational interests in using the data. Another transmission principle is that the sending district and recipient contractor enter into a confidentiality agreement for using the student information to ensure it is only used for the purpose of the agreed-upon service. These policies do not provide further details about what these written agreements will contain.

Using Contextual Integrity for Policy Creation and Adoption

The non-BoardDocs policies do not specifically address student data use within current educational technology practices. Still, principles from the contextual integrity framework can aid in making these policies more relevant and applicable. Nissenbaum writes that the CI framework can operate as a decision-making tool for the flow of information within a context. The framework is valuable when significant components of the context change, like the dynamic growth of educational technology and the increasing capability to create, analyze, and disseminate information about students. Board members and school leaders need not be contextual integrity scholars to benefit from this framework as they adopt policies and procedures for student data use within modern educational technology systems.

When considering these potential policy and procedural changes, the first step is understanding the current context of the information flow (Nissenbaum, 2010). For these policies, the larger context is not changing as the setting is still within schools providing educational services to the students. The social norms also remain the same. Parents and staff members still value education for students and remain committed to their privacy.

The next critical step for school leaders is to examine if there are changes in the actors involved in the information flow. The sender of information is still the school district, and the subjects of the data are still students. The significant change is that the recipients now include third-party companies using student data as part of an educational service provided to the district. The information attributes may also change as new data types are created and collected to utilize the service provided.

The most significant changes for school leaders to consider and account for within these new policies would be the transmission principles or required conditions for student data disclosure. Written agreements should specify these transmission principles with the receiving entities, and the board policies should provide detailed expectations about the use and safekeeping of student information. Like in the BoardDocs policies, the agreements should clearly outline what data will be used, how it will be used, who has access to the information, and a timeline for the service activities. Additionally, the agreement should address the security practices the recipients have in place and what will happen to the student data after the agreed-upon services.

Finally, Nissenbaum urges those involved to look for potential concerns that may be present in the new information flow practices. In the context of sharing student data with third parties, that concern is likely with parent expectations and awareness for who has access to their

children's personal information. Transparent communication from the district can address concerns by letting parents know what student data is shared, who is receiving the information, how it is used, and the agreements in place to ensure the appropriate use and safeguarding of the data.

Summary of Student Records Policies

Since there is no detailed state legislation in Wisconsin for the protection of student data, district leaders implement local board policies to meet federal regulations requirements and guide the district's daily operations when using student information. By analyzing the student records sections of the BoardDocs policies through Nissenbaum's contextual integrity framework, I have shown how these policies specify the district stakeholders' expectations when sharing student data with outside entities. These policies identify the CI contexts, actors, information attributes, and transmission principles. Additionally, these BoardDocs policies are fitting for using student data created, collected, analyzed, and disseminated through current technology tools and resources. I have also described how school leaders can use the contextual integrity framework to update student records policies and make them relevant to modern uses of educational technology resources and student data.

Federal Student Data Privacy Regulations

Wisconsin statute 118.125 does not provide detailed guidance for treating pupil records and other student information. The statute requires that records are kept confidential and then tasks local school boards to adopt policies to address the appropriate storage and disclosure procedures for student information. Because of this lack of state regulation, establishing local policies in line with federal regulations is central to the appropriate safekeeping and use of

student data. My interpretation of the second research question focuses on how these policies address federal regulations in the context of modern educational technology tools.

Family Education Rights and Privacy Act

The primary expectations outlined by FERPA regulation are parents' rights to access the records of their children, the opportunity to amend the records and control with disclosure of student PII found within those records (USDOE, 2022). This study focuses on this last component of disclosure as it is relevant for situations where student data is used by or created through educational technology. Since FERPA focuses on student records, most of the FERPA references were found within the district student records policies in this study. Therefore, the findings' significance for addressing FERPA is like what was explained in the first research question above. The regulation is referenced within the board policies of 23 of the districts in this study, and 15 of these policy books make clear and detailed connections with FERPA when there are situations where student data is disclosed to outside entities like contracted vendors and other organizations using student data. As stated in the student records discussion, these 15 districts all use the BoardDocs policy service.

There are two other policies aside from the BoardDocs policies that make a less detailed connection between FERPA and student data sharing and use the same policy language. That language reads:

> The District will make available the Students' directory data and other student and student records to certain independent contractors and vendors, including, but not limited to, bus companies, assessment services, and database reporting services, who have been determined by the school board to have legitimate educational interests, including safety interests, in the records. The District will enter into confidentiality agreements with such

independent contractors and vendors before sharing any student or student records to ensure that the records are only used in connection with the contracted services provided. The policy references contractors, vendors, and assessment services directly relevant to student data use and educational technology. The policy states that these districts will use confidentiality agreements to ensure the data is used according to the contract. Still, no other details for third-party agreements are provided within this policy section or elsewhere in the policy books of these districts. The BoardDocs policies clearly state that FERPA compliance is expected in these data use agreements with vendors and other third parties.

Outside of these two examples and the BoardDocs policies, the FERPA references within these policies outline the traditional practices of transferring documents to other districts and other local entities. These traditional practices are essential as student records do need to move from one legitimate party to another confidentially. Still, these policies appear to be out of step with current uses of educational data within powerful technology tools. I assume that these districts are using modern technology tools and student data is being shared for the benefit of the student and the district, but the policy language present at the time of this study does not address these practices.

Recommendations for FERPA Policies. Since the primary focus of these student records policies is on the expectations of FERPA, the recommendations are the same. The BoardDocs policies have detailed procedures to address FERPA requirements when student data is shared with third-party companies providing educational technology and data assessment services. The policies that are not as detailed should be updated with language that addresses the contexts where digital student data is shared with third-party companies and organizations

providing educational and data services. This process can be aided by using the contextual integrity components described previously.

Another recommendation I offer is for school leaders to understand the four common parent consent exceptions outlined in FERPA. The first exception is districts do not need parental consent to disclose directory information, but they do need to inform parents about what information is designated in this category. This exception was commonly outlined in the records policies in this study, but it is a key concept that leaders should know.

The second exception is that student information can be shared without parental consent with those designated as school officials and have a legitimate interest in accessing student data. The *school official exception* is how districts can share student data, without parent consent, with vendors and contractors providing educational technology and data assessment services. Representatives from these companies can be classified as school officials to gain access to student information. Districts must provide criteria on who is a school official and what constitutes the legitimate interest in their annual parent notifications. These terms were found in many of the policies in this study. Still, leaders should understand these terms and procedures well enough to explain these ideas beyond the often confusing policy language syntax.

The third exception leaders should know concerns studies that use student PII to evaluate school programs and services. The last exception is similar to audits and evaluations conducted by state and federal organizations to ensure district program compliance. The district should establish written agreements with the receiving institution about the needed data for each of these exceptions. The BoardDocs student records policies are good examples of what these written agreements address. However, school leaders need to understand the FERPA requirements and how their local policies satisfy them.

These four exceptions can be applied in contexts where digital data is shared in modern educational technology systems, but they are relevant in traditional records disclosure situations. The key is for leaders to understand these general concepts and know how to apply them in various scenarios when it is necessary to share student information.

Children's Online Privacy Protection Act

References to COPPA were found in the policy books of 18 districts in this study. Fourteen of those policies are the ones using the BoardDocs service. Like the student records policies and the FERPA procedures, the BoardDocs policies clearly describe the contexts where COPPA is required for using technology tools.

Before further explanation of those policies, I will highlight two other district policy sections which provide clear guidance to district staff on the COPPA requirement and student use of educational technology. The Holmen and La Crosse school districts state within their AUPs that staff members have permission to allow their students to create accounts and use web-based services for educational reasons. The policy requirement for doing this is that the accounts need to be created in compliance with COPPA. To be COPPA compliant, users must be 13 years or older. The policy clearly states this age expectation and directs staff members to work with the student's parents if they are under 13. These two policies adequately address one of the common criticisms of COPPA and how it applies in school settings where parents are often not available to be informed of the terms of service when students create accounts for online education services (Federal Trade Commission, 2022).

The COPPA references from the BoardDocs policies come from the *web content, apps, and services* sections. These policies do not address the parent involvement requirement like discussed in the previous paragraph. Still, they clearly define when the COPPA regulation needs

to be applied when working with students and technology. In these policies, staff members and students can create content and tools using district technology resources, and their work must comply with COPPA. In addition to the staff and student-created content, the policies also recognize that services and content created by third parties will be used within the district and linked on district web pages and link hubs. These services developed by vendors, contractors, and outside companies must also be COPPA-compliant before being shared through district pages. Finally, these policies describe the process staff members must follow before using an online service or app with their students. Staff members are required to show verification to one of the school administrators that the educational resource they would like to use is compliant with COPPA and FERPA. These COPPA references clearly state expectations for staff members and describe the educational situations when COPPA compliance is applicable and required.

Recommendations for COPPA Policies. What is interesting and complicated about COPPA is that the regulation was created to limit operators of websites and other technology companies with how they collect and use data from users under the age of 13. FERPA and PPRA were written to regulate school use of student information and is enforced by the U.S. Department of Education. In contrast, the Federal Trade Commission enforces COPPA among private companies and non-education entities. Schools have no direct COPPA obligations but contract with educational technology companies to provide valuable services to educators and students. In these service arrangements, it is legally permissible for school staff to consent for student data to be collected and used by the technology company for educational activity purposes.

While it is legal for staff to give this consent on behalf of the parents, I would suggest that schools keep parents informed of the technology services provided in their children's

education and the specific student information used with these services. The BoardDocs policies state that apps and services must be COPPA-compliant, but there is no mention of keeping parents informed about the services and what student data is collected by these services. Of all the policies examined in this study, only La Crosse and Holmen school districts address communication with parents when creating accounts with third-party educational services companies. Districts are not required under COPPA to communicate with parents. Still, it would be beneficial for them to do so to keep parents informed about the educational technology programs used and the agreements that districts have with these companies for the appropriate use of student information.

The FTC recommends that districts establish procedures to verify the appropriateness of these service providers rather than leaving the consent to individual staff members. The BoardDocs policies in this study state that teachers must verify with an administrator that the app or service is COPPA, CIPA, and FERPA compliant. However, these policies do not provide any additional guidance regarding what constitutes compliance. One suggestion would be to provide policy language like in the BoardDocs student records sections for written agreements with third parties. A written agreement with these companies would describe what student information is shared, the specific limited use of the data, and which personnel can access the student information. Additionally, the written agreement would state the need for the company's security capabilities and the procedures for destroying student data after the service.

Protection of Pupil Rights Act

This regulation involves the rights of parents and students when surveys, audits, and other evaluations collect specified categories of sensitive information. These categories are:

- mental or psychological problems of the student or his/her family;

- sex behavior or attitudes;
- illegal, anti-social, self-incriminating or demeaning behavior;
- critical appraisals of other individuals with whom respondents have close family relationships;
- legally recognized privileged and analogous relationships, such as those of lawyers, physicians, and ministers;
- religious practices, affiliations, or beliefs of the student or his/her parents; or
- income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such a program).

When surveys collect information in any of these categories, the PPRA regulation requires the district to notify parents before the event so they can inspect the information collection instruments. In addition, parents have the right through PPRA to opt their children out of participation in any collection activity involving the information categories above. All 15 of the BoardDocs policies and five additional policies specifically reference this law's notification, inspection, and opt-out requirements. These 20 policies also list these eight categories of information. The only significant difference between the BoardDocs policies and the other five is that the BoardDocs policies have requirements for data agreements be used with the organization administering the survey. These are the same agreements described previously in the student records discussion above.

Recommendations for PPRA Policies. The 20 policies in this study describing parents' rights and school responsibilities all address the PPRA rule's major components. The PPRA guidance for educational organizations does not require data stewardship plans when sharing student information with the entities conducting the surveys and audits. Still, I would

recommend this practice since it is already an expectation for sharing student records under FERPA. The student information in these surveys is not considered educational records, but the concept is similar. Personal information from students is shared with third-party entities. Regardless of which federal regulation applies, districts can build trust with parents and students by informing them of the expectations that are in place with the recipients of student data.

Summary of Federal Student Data Privacy Regulations

Of the 25 districts with policies available for this study, 23 refer to FERPA within their policy books. Of those 23 districts, the 15 BoardDocs policies provide detailed procedures for disclosing student data relevant to modern educational technology use and working with outside contractors and services. The other districts' policies primarily describe traditional types of student record sharing. The COPPA regulation was clearly addressed with detailed procedures in 17 of the district policies in this study. Still, I recommend that districts inform parents about agreements they have in place with companies providing educational services. Policies of 20 districts thoroughly describe the PPRA law, but increased parent communication and established written agreements with the data recipients are suggested areas for improvement.

But Are These Policies Effective?

Before moving into the last research question about the role of leadership with the board policies, I will provide a practical examination of how well the policies might guide the work of district staff to protect student information. Question 1 examined the general approach to data privacy in student records policies, and the second question specifically focused on federal regulations for using and sharing student information. The district guidelines using the Neola consultation service provided enough detail to describe how student data should be used in modern educational technology services. The BoardDocs policies also provide explicit language

to show compliance with COPPA, FERPA, and PPRA federal regulations. While the policy language adequately addresses data use and demonstrates federal compliance, a typical staff member would not find the clear and direct guidance they need to know they are appropriately using and protecting student information.

The language within these compliant policies is very detailed to show compliance with federal regulations. The wording and structure are technical, often reflecting the same language in the federal rules. Additionally, the policies address the federal laws in multiple sections of the policy book, which contains hundreds of policies accounting for nearly all operational aspects of the district. Unless one were remarkably familiar with the organization of the policy book, it would take considerable effort to find all the relevant sections needed to answer everyday data use and disclosure questions.

However, this does not mean the policy itself is inadequate. Research from the National School Board Association (Dervarics & O'Brien, 2019) found that one of the characteristics of effective school boards is that they develop and adopt student-focused policies and spend less time on the operational aspects of the district. First, school boards set the stage for *what* should happen with their policies. Boards then allow and equip school leaders and staff to develop *how* that work is implemented. Then, the professional education staff creates plans and procedures to satisfy the guiding policies.

Policies become operational through the creation of administrative guidelines and procedures. Functional guideline documents are vital for meeting the expectations of these policies, but it is challenging for local school leaders to create these procedural documents on their own. The Neola company offers a service to their district customers and states on their web page, “Our superintendent-approved guidelines/procedures give districts direction on how to

implement the related policy (2023).” Since remote professional policy consultants and attorneys write these policies, the administrative guideline service seems to be an essential step for the policy implementation process. However, of the 15 districts in this study using the Neola BoardDocs policy service, only three have administrative guidelines shared on their board policy pages. Further, the procedural guidelines in these three districts generally repeat the same technical language found in the board policies. As a result, they do not provide the needed support to staff members trying to meet the expectations of the local policies and the federal regulations they address.

The same barrier of technical legal language exists for parents who want to understand district policies and procedures for data use and protection. Parents have access to the board policies as public records but would find the same challenges staff members do with locating and comprehending the policies. Federal regulations require districts to notify parents about their rights and district procedures for student records and information. The common approach among the districts in this study is to provide an *annual notices* document with dozens of links for various required notifications. These notices also contain dense legal language or the same language from the board policy.

These complex policies for intricate data privacy issues are an opportunity for school leaders to work with the board, parents, and other community stakeholders to develop needed guidelines and communication methods. In addition, they can identify common questions and information needs to support utilizing innovative technology resources while preserving student privacy. This collaborative effort should include resources from the policy consultation company which wrote the guidelines. The USDOE’s Privacy Technical Assistance Center also provides numerous support documents for school leaders, parents, researchers, and vendors.

This study has found that the policies from the districts using the Neola consultation service provide a framework for compliance with federal regulations for student data protection. However, additional work is necessary to create procedural documents to guide the work of district staff members. There is also a need to create clearer notifications to parents about how student data is used and shared. These additional resources can support these policies' daily implementation and effectively communicate procedures with parents and other community stakeholders.

Leading Data Privacy Policies

The interpretations of the findings will focus on the roles of the superintendent, principals, and technology directors in leading the student data privacy policies explored in this study. Scholarship shows that leadership is vital for successfully implementing and using educational technology (Anderson & Dexter, 2005; Bjork, 1993; Dexter & Richardson, 2020; Levin & Schrum, 2012; McLeod et al., 2015). The responsibilities of school leaders were evident throughout these policies and will be explained in this section.

Superintendent Responsibilities

These policies ask superintendents to create guidelines and develop procedures for many functions regarding the use of student data and educational technology. Policy implementation can be complex, and as superintendents bring policy to life, they must consider the impact these procedures will have on the stakeholders within their school communities (Kingdon, 2003; Young & Lewis, 2015). These leaders are tasked with notifying the school community about district procedures for the use of student data and for helping parents understand their rights provided by federal regulations. In addition, superintendents work with parents concerned about student records' privacy or desire to amend those records. District administrators are also

accountable for creating response plans and communications in case of an unauthorized breach of district information. These types of communication and relationship-building about district procedures, especially with parents and community members, are practices associated with effective leadership (Hitt & Tucker, 2016).

Superintendents also establish procedures for appropriate data storage methods, disclosure procedures, and retention timelines. In addition, they develop guidelines to support the expectations in acceptable use policies for students and staff. These top administrators also oversee the implementation of district web filtering and monitoring systems. Finally, superintendents lead risk assessments to ensure procedures are in place for the appropriate use of student data. These activities may seem managerial and not necessarily visionary, but having these procedures in place is necessary for compliance and the overall well-being of the district (Dexter & Richardson, 2020; Richardson & Sterrett, 2018; Rost, 1993; Sauers et al., 2014).

These policies also ask superintendents to demonstrate their collaborative abilities as they work with key district members to develop technology acquisition and implementation plans (Dexter & Richardson, 2020; Richardson et al., 2015; Waters & Marzano, 2006). In addition, district administrators ensure all staff members receive the training necessary to ensure compliance with local policies and the federal regulations referenced in those policies. Finally, modeling and promoting ethical behavior and regulatory compliance is another skill exhibited by effective school leaders (Hitt & Tucker, 2016; International Society for Technology Education, 2022; Lee et al., 2016; National Association of Secondary School Principals, 2022).

Implications for Superintendent Practice. The responsibilities described for superintendents in the previous sections are like what is present within the research for effective educational leadership and technology leadership. They share visions, communicate with

stakeholders, and create and support educational activities within their districts. These responsibilities are similar to effective leadership within other district operations areas. However, data privacy may be more challenging because of the dynamic nature of educational technology and how student data is used. These resources and tools continue to improve, become more efficient, provide powerful educational and instructional opportunities, and use and create student data in new ways.

District leaders should ensure that the appropriate use of data privacy is a component of technology training for staff members. School leaders should develop a foundational knowledge of federal regulations, especially modern applications of FERPA. Superintendents should ensure the training for staff members, students, and parents focus on the practical use of data within educational technology programs. District administrators can lead educational efforts for their staff members by making all aware of how federal, state, and local policies address the expected use of student data. Many of the policies within this study outline the expected process for choosing and implementing instructional technology. The internal training efforts of superintendents and other leaders should highlight these processes and show support for using effective and compliant technology tools.

It may be challenging for district administrators to closely track the growth of technology resources and their powerful use of student data. Still, these leaders would benefit from developing a general understanding of data governance policies. The technology will continue to change, but the concepts within data governance are more stable and appropriate for superintendents to comprehend and lead. Leaders should establish systems within their districts to accurately record all types of student data collected, the purpose of use, where the information is stored, who has access, and the timeline for the service and destruction of the data. These

governance practices connect district visions and data use and plan for risk assessments to ensure the security of student information and other sensitive district data. Transparency is a crucial part of data governance, and superintendents should make the data use known to all stakeholders within the school community, especially students and their parents. This type of clear communication is a chance to show how the district provides compelling educational experiences through technology and establishes trust with parents by demonstrating the appropriate use and security of student information.

Wisconsin superintendents should also use their influence as community leaders to work with state lawmakers to provide more detailed regulations for using student data. As seen in this study, comprehensive policies account for data use within educational technology tools. Still, the appropriate use and safekeeping of student data should not primarily depend on the type of policy consultation service a district employs. The current Wisconsin statutes allow for a lot of local control by district school boards, but I don't see how local control benefits a subject like student information. State regulations would provide more guidance to districts, help bridge gaps among the federal data laws, and place more responsibility on companies providing technology and data services to school districts. School superintendents and school board leaders should work with state lawmakers and the Department of Public Instruction leaders to ensure legal and procedural support for the appropriate use of technology and student data.

Principal Responsibilities

The most common responsibility of principals within these policies is to train their staff members to be knowledgeable about the appropriate use of technology resources and student data protection. Providing this training and support to staff members provides them with the background and ability to educate students about using technology resources within the school.

In addition, the training for all these members leads to the effective use of technology and is critical to the ethical use of these resources and compliance with local policies and federal regulations (Dexter & Richardson, 2020; ISTE, 2022; NASSP, 2022; Richardson & Sterrett, 2018; Sauers, 2014).

These policies show how principals should know the federal regulations and policies to lead disclosure requests with student records. In addition, they communicate and work with parents regarding records transfers and the release of directory information. Principals also support parents who have questions about data collection and want to inspect the related tools. Collaborative and communicative work with parents are practices of influential school leaders (Hitt & Tucker, 2016).

Implications for Principal Practice. From my experience as a former school principal and as seen throughout the policies within this study, principals are responsible for the daily educational activities that occur within their schools. The training of staff and education of students are included in these activities and are vital practices for ensuring the protection and appropriate use of student information. The Black River Falls policies state that "trained employees will help provide the best defense" for avoiding information breaches and unintentional student data disclosures.

Superintendents and policies may outline the expectations for training, but principals are the leaders to ensure the training is provided and continually followed. The student AUPs outline expected and prohibited technology practices and commonly mention the building administrators as the primary supporters and enforcers of these policies. Many technology-use policies in this study clearly state that students will receive education about the dangers of disclosing personal information in online environments, whether or not the disclosure was intentional. School

principals and staff can focus on these privacy concepts as life skills, not compliance obligations, to show students the relevance of data privacy and control even after they complete their education. The student's data collection and use knowledge is a crucial concept of being a digital citizen, and principals can ensure these skills are taught and practiced across all school curriculum areas.

Principals are the instructional leaders of their schools and are responsible for ensuring the appropriate use of technology resources. Principals should be involved with selecting instructional resources, including technology, and ensure that the uses of these resources align with the goals and needs of the school and are in compliance with district policies for resource selection. Many of the policies examined in this study name the principal as the leader of the vetting process for apps and services to ensure they comply with FERPA and other federal regulations. Building leaders should have at least a working knowledge of these regulations, especially how they apply to technology services provided by private companies and third parties.

Beyond the working knowledge, principals should develop a deeper understanding of federal regulations and best practices provided by professional organizations and student privacy advocacy groups. Principals lead the daily work with the technology tools and services which enable instruction, learning, and communication. They should continue at the forefront of adopting educational technology resources and lead the protection and appropriate use of student data.

Responsibilities of Directors of Technology

IT directors play a vital role in verifying apps and services that staff members want to use with their students. In addition, they must ensure they comply with board policies and federal

regulations for student privacy. Another procedural role they have is to make changes to the district filtering and monitoring technology to ensure compliance with federal laws regarding access to inappropriate web content. These compliance enforcement and support roles are known to be key practices for appropriately using student data (ISTE, 2022; NASSP, 2022). These directors support the work of superintendents with implementing and enforcing acceptable use policies for all members of the school community. IT directors also provide individual support and training for staff members who have questions or need assistance with information security processes expected in schools. These directors demonstrate their policy implementation and professional development abilities as they support their districts in these two areas (Dexter & Richardson, 2020; Richardson & Sterrett, 2018; Sauers et al., 2014; Young & Lewis, 2015).

Implications for IT Professionals. The responsibilities of IT staff outlined in the previous paragraph and Chapter 4 are only those relating to student data use and privacy. Beyond the topic of this study, these technology professionals are also responsible for the budgeting, acquisition, installation, maintenance, problem-solving, and replacement of user devices and infrastructure resources across the district. Their work also supports the non-instructional technology needs of the district for food service, transportation, and financial management.

Over the past two decades, the educational technology boom dramatically increased the number of devices used within schools. Technology leaders and their staff have been challenged to keep up with these new hardware and software resources to support instruction and the overall operation of schools. Traditionally, IT leaders were asked to lead compliance issues with federal regulations, copyright concerns, and technology use policies for staff and students. While there have been shifts to share these responsibilities with other educational leaders within school

districts, adopting new technology and the uncertainty of student data practices can concern IT leaders. This concern is especially evident when they have limited time to understand the privacy policy implications that may go with these new tools. In light of the other demands upon these directors, it may be understandably tempting to advocate against implementing the new resources. Instead, IT leaders should communicate clearly to superintendents and district-level leaders about the real demands and challenges within technology departments. Student data privacy is a technology concern that should be shared with instructional and policy leaders within schools.

Implications for Education Leadership Preparation Programs

Education training programs will continue to be a primary means for ensuring current and future school leaders can balance using innovative technology resources and protecting student data. I would advocate for an increased emphasis on policy comprehension and creation within these programs to help leaders understand how policies can guide effective technology use and data protection.

Coursework should include a strong foundation in data privacy, basic cybersecurity, and information management to ensure future school leaders are familiar with the concepts and best practices of data protection. In addition, these programs should include risk assessment, prevention, and risk mitigation with data breaches. Foundational learning objectives should also ensure school leaders are familiar with relevant state and federal legislation such as FERPA, COPPA, and PPRA and how they apply to modern uses of innovative technology. Leaders should also learn model state regulations like California's Student Online Personal Information Protection Act (SOPIPA) and the Europan Union's General Data Protection Regulation (GDPR).

Leadership preparation programs typically include expected outcomes for policy development and evaluation. Within these policy courses, future leaders can develop their practical skills with the topic by evaluating, drafting, and revising actual board policies which address how districts share data with third-party educational technology companies. In addition, these practical exercises should include discussing ethical issues with data-sharing and prioritizing the rights of students within technical systems.

Communication and collaboration skills can also be developed and practiced with data protection in mind. The policy development process involves many stakeholders, including parents, students, board members, and other education staff. Leaders should be able to recognize how to communicate with all of these groups effectively to share basic information about programs, solve conflicts, and remediate issues with data protection.

These development programs can also support leaders by helping them recognize the rapid evolution of technology and the changing nature of best practices and regulations that follow these resource improvements. Leadership preparation programs typically include continuous improvement processes, and student data protection can be included in these studies. Future school leaders can learn how to review policies and regulations to address data sharing and security. They can also develop plans to monitor the performance of third-party entities using student data for district programs.

In conclusion, education training programs are vital for equipping current and future school leaders with the knowledge and skills to balance innovative technology use and student data protection. These programs should emphasize policy comprehension and creation, including a solid foundation in data privacy and relevant legislation. Furthermore, leadership preparation programs should encompass practical policy development exercises and foster communication

and collaboration skills among various stakeholders. Finally, by staying up-to-date with the rapid evolution of technology and continuously improving practices, these programs can effectively prepare school leaders to address data sharing and security concerns.

Summary of Leadership Responsibilities

School leaders are responsible for appropriately using and safeguarding student data within these policies. They lead policy implementation, develop systems to satisfy policy and regulatory requirements, provide professional development, and effectively communicate with all school community members. These skills are essential for their work to support the appropriate use of student information, but they are also vital for the overall educational leadership they provide.

Recommendations for Future Research

The analytical approach for this study was primarily focused on content, but additional policy analysis methods could be used to explore these policy documents. A critical policy analytic approach could explore power differences with how these policies impact different populations of students and parents within the same school district. For example, these policies state that parents have rights expressed within federal regulations to inspect collection instruments used to get sensitive information from students. Districts notify parents about their rights, but what are the barriers for parents to understand and act on their rights? A critical approach could be used to examine student acceptable-use policies to explore potential differences in how they impact students from different family backgrounds and the primary language spoken at home. A discursive analytical approach with these policy documents could also provide insights into the value the district places on the rights of parents in the context of the use of evolving educational technology resources.

The data sources for this study were strictly board policy books. Still, I recognize from my experience as a former school principal that there are often differences between what is expressed in board policy and what happens in practice. Broadening the data sources and methodological approach would expand the understanding of *how* school leaders implement the procedures expressed within these policies. For example, one could use a case study approach to explore potential differences in policy implementation between districts using different policy consultation and publication services. Comparisons could also be made among the districts using the same policy service. In addition, examining procedural documents not found in board policies and interviews with school leaders could provide additional information about policy implementation.

Another intriguing topic that emerged from the focus on the responsibilities of school leaders is these leaders' knowledge of the federal regulations which address student data privacy. Additionally, what resources do these leaders use to support their implementation of the rules found in their board policies? The patchwork of federal, state, and local regulations for student information is challenging, so it would be interesting to examine more precisely what leaders understand as they support their district stakeholders.

Limitations

While I tried to remain objective and aware of my pro-technology biases as a researcher, I recognize my experiences with technology and district policies have influenced my perspective on the intersection between policy and practice. My initial interest in federal regulations for student data began before I started the doctoral program, leading to this research. My eagerness to implement new educational technology resources as a school leader often conflicted with the caution and limited resources of the school technology staff. While this conflict sparked my

interest in policy and regulations, I have tried to retain needed objectivity by relying on actual excerpts from these board policies as data sources.

Additionally, this study focused on the board policies of 26 districts within one educational service agency in Wisconsin. Among these districts, 23 made their entire policy books available for my research. Even though Wisconsin's public records law stipulates that schools provide documents like board policies to anyone who requests them, I did not aggressively pursue the collection of these documents from three of the districts which provided few or none. Instead, I made my initial requests via email and followed up twice before moving on with the policies I had already collected. While I do not attempt to generalize these results to the whole service agency area or beyond, I assume that the policies not provided by these other districts might contain significantly different approaches to student data privacy.

Finally, as noted previously, the primary focus on board policies as data sources may not provide the entire approach to how districts address student privacy. I am confident that my study is thorough and accurate with what is present within these policies, but I recognize that additional data sources would add to the knowledge base. Procedural documents that are not part of the policy books likely exist, and these districts may have practices to address the security and use of student information. I also know that interviews with school leaders about data privacy practices would provide abundant information to add to the body of research.

Conclusion

In this chapter, I reviewed the study's key findings and then provided interpretations and practical implications based on these findings. In Wisconsin, there are no state statutes that provide detailed guidelines for the protection of student data. Therefore, school leaders depend on their local board policies to address the requirements of federal regulations for student data

privacy requirements as they use educational technology and work with entities that provide services to the schools. In addition to federal compliance, these policies outline district beliefs and responsibilities to protect student information as schools work with third parties that provide services for teaching and learning.

In this study, I noted that districts using the BoardDocs policy service had student records sections that provided detailed policies for using student data when working with outside entities for surveys, audits, and evaluations. I used the contextual integrity framework to describe the components of expected information flows when using student information. The framework helped demonstrate which policies apply to student data-use in modern technology systems. I also showed how the CI framework could help adapt traditional records policies to account for current data use within innovative technology systems. I also posit that the districts using the Neola policy service provide compliant policies when describing the requirements of the federal regulations Family Educational Rights and Privacy Act and the Children's Online Privacy Protection Act. The district policies in this study largely provided appropriate policy language for addressing the Protection of Pupil Rights Amendment requirements. This study also identified opportunities for school leaders, board members, and parents to work together to increase procedural implementation and communication with district stakeholders. Finally, leaders have many responsibilities outlined in these policies regarding the appropriate use of student data. Effective educational leadership practices identified in previous research are appropriate for fulfilling these responsibilities with student data.

APPENDIX A: IRB REVIEW

University of Kentucky | Office of Research Integrity
IRB, RDRC

XX

IRB Number:
74860

TO: Curtis Rees, Ph. D.
Educational Leadership Studies
PI phone #: 6083173747

PI E-mail: curt.rees@uky.edu

FROM: Chairperson/Vice Chairperson/Office of Research Integrity
Nonmedical Institutional Review Board (IRB)

SUBJECT: IRB Review

DATE: 9/26/2022

On 9/23/2022, a designated official reviewed your proposal entitled:

School district policies regarding student data privacy

The designated official determined that your proposal does not meet the federal definition of human subjects, "a living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information" [45 CFR 46.102(f)], and thus does not need IRB review.

Should any facts change please contact ORI as that may render the protocol eligible for IRB review and approval.

If you have any questions regarding the designated official's decision or need additional information, please contact the Office of Research Integrity at 859-257-9084.

References

Abbott, H. (2020). *Gatekeepers of student data: A comparative case study of requests for student data at decentralized research universities* (Publication Number 28260932) [Ed.D., Northeastern University]. ProQuest Dissertations & Theses Global; Social Science Premium Collection. Ann Arbor.

Abilock, R., & Abilock, D. (2016). I agree, but do I know? Privacy and student data. *Knowledge Quest : Journal of the American Association of School Librarians.*, *44*(4), 10-21. https://files.eric.ed.gov/fulltext/EJ1092205.pdf

Ahn, J., Campos, F., Nguyen, H., Hays, M., & Morrison, J. (2021). *Co-designing for privacy, transparency, and trust in K-12 learning analytics.* LAK21: 11th International Learning Analytics and Knowledge Conference,

Alliance for Excellent Education. (2022). *Future ready district leaders*. Retrieved July 17, 2022 from https://futureready.org/wp-content/uploads/2020/04/district_leader_flyer_8.10.17.pdf

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*(3), 377-387.

American Association of School Administrators. (2022). *AASA belief and position statements*. Retrieved July 17, 2022 from https://www.aasa.org/uploadedFiles/About/AASA_Bylaws/Belief-Position-Statements.pdf

Anderson, J. (2020). The coronavirus pandemic is reshaping education. *Quartz.com*. https://qz.com/1826369/how-coronavirus-is-changing-education/

Anderson, R. (2019). The emergence of data privacy conversations and state responses. *Protecting students, advancing data: A series on data privacy and security in higher education*. https://vtechworks.lib.vt.edu/bitstream/handle/10919/92664/DataPrivacyLouisiana.pdf?sequence=1

Anderson, R. (2022, July 17, 2022). Student data privacy in 2022: Cutting through the noise. *DQC Blog*. https://dataqualitycampaign.org/cutting-through-the-noise/

Anderson, R., & Dexter, S. (2005). School technology leadership: An empirical investigation of prevalence and effect. *Educational Administration Quarterly*, *41*(1), 49-82. https://doi.org/10.1177/0013161X04269517

Anshari, M., Hamdan, M., Ahmad, N., Ali, E., & Haidi, H. (2022). COVID-19, artificial intelligence, ethical challenges and policy implications. *Ai & Society*, 1-14.

Apthorpe, N., Varghese, S., & Feamster, N. (2019). *Evaluating the contextual integrity of privacy regulation: Parents' IoT toy privacy norms versus COPPA.* 28th USENIX Security Symposium (USENIX Security 19),

Arnett, T. (2021). Carpe diem: Convert pandemic struggles into student-centered learning. *Clayton Christensen Institute for Disruptive Innovation*.

Association of Wisconsin School Administrators. (2022). *AWSA home page*. Association of Wisconsin School Administrators. Retrieved April 23, 2020 from https://www.awsa.org/

Aung, Y. Y., Wong, D. C., & Ting, D. S. (2021). The promise of artificial intelligence: a review of the opportunities and challenges of artificial intelligence in healthcare. *British medical bulletin*, *139*(1), 4-15.

Babler, J., Horbath, F., Huang, D., Martin, E., Prichard, M., & Smith, N. (2017). *Building effective communications around student data privacy: An analysis of select K-12 edtech companies.* Heinz College Systems Synthesis, Pittsburgh, PA. https://fpf.org/wp-content/uploads/2017/11/Building-Effective-Communications-around-Student-Data-Privacy-1.pdf

Bagchi, K. J., Bannan, C., & Gambhir, R. (2021). *Working and learning during the pandemic: Surveillance of students and employees is not the cure*. http://newamerica.org/oti/reports/working-and-learning-during-the-pandemic/

Bailey, J. P., & Hess, F. M. (2020). A blueprint for back to school. *American Enterprise Institute*. http://www.jstor.com/stable/resrep24606

Baldridge, S. (1995). Models for school board policy development: Rationalism, empiricism and the new science. *Brigham Young University Education and Law Journal*, *1995*(1), 43-61. https://digitalcommons.law.byu.edu/elj/vol1995/iss1/4/

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). *Privacy and contextual integrity: Framework and applications.* 2006 IEEE Symposium on Security and Privacy,

Bathon, J. (2013a). The fine print on cloud computing. *T H E Journal*, *40*(9), 23-26.

Bathon, J. (2013b). How little data breaches cause big problems. *T H E Journal*, *40*(10), 26-29.

Bathon, J. (2013c). One student, one device, and a thousand laws. *T H E Journal*, *40*(8), 24-25.

Bergelson, V. (2003). It's personal but is it mine: Toward property rights in personal information. *UC Davis L. Rev.*, *37*, 379.

Berger, M., Kuang, M., Jerry, L., & Freund, D. (2022). Impact of the coronavirus (COVID-19) pandemic on public and private elementary and secondary education in the United States (preliminary data): Results from the 2020-21 National Teacher and Principal Survey

(NTPS). First Look. NCES 2022-019. *National Center for Education Statistics*. https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2022019

Birnhack, M., & Perry-Hazan, L. (2020). School surveillance in context: High school students' perspectives on CCTV, privacy, and security. *Youth & Society*, *52*(7), 1312-1330.

Bjork, L., & Gurley, D. K. (2003). Superintendents as transformative leaders: Schools as learning communities and as communities of learners. *Journal of Thought*, *38*(4), 37-78. http://www.jstor.org/stable/42589764

Bjork, L., & Lindle, J. C. (2001). Superintendents and interest groups. *Educational Policy*, *15*(1), 76-91. https://doi.org/10.1177/0895904801015001005

Bjork, L. G. (1993). Effective schools–effective superintendents: The emerging instructional leadership role. *Journal of School Leadership*, *3*(3), 246-259. https://doi.org/10.1177/105268469300300303

Black Jr, W. L., & Shaver, E. A. (2019). The first amendment, social media, and the public schools: Emergent themes and unanswered questions. *Nev. LJ*, *20*, 1.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal 9*(2), 27-40. https://doi.org/10.3316/QRJ0902027

Braman, S. (1989). Defining information: an approach for policymakers. *Telecommunications Policy 13*(3), 233-242.

Bratman, B. (2002). Brandeis and Warren's the Right to Privacy and the birth of the right to privacy. *Tennessee Law Review*, *69*(3), 623-652. https://heinonline.org/HOL/P?h=hein.journals/tenn69&i=634

Brewer, D. J., & Picus, L. (2014). School boards. In D. J. Brewer & L. O. Picus (Eds.), *Encyclopedia of Education, Economics, and Finance*. SAGE Publications, Inc. https://doi.org/10.4135/9781483346595.n236

Bruno, S., Feldman, J., Todd, E., & Fultz, E. (2022). *The Kids Online Safety Act*. Reedsmith.com. Retrieved July 16, 2022 from https://www.reedsmith.com/en/perspectives/2022/02/the-kids-online-safety-act

Bulger, M., McCormick, P., & Pitcan, M. (2017). *The legacy of InBloom* (Enabling Connected Learning, Issue. https://datasociety.net/pubs/ecl/InBloom_feb_2017.pdf

Burns, J. M. (1978). *Leadership*. Harper & Row.

Bushweller, K., & Lloyd, S. (2021). How the pandemic is shaping K-12 education (in charts). *Education Week*. https://www.edweek.org/leadership/how-the-pandemic-is-shaping-k-12-education-in-charts/2021/04

Cardno, C. (2018). Policy document analysis: A practical educational leadership tool and a qualitative research method. *Educational Administration: Theory and Practice*, *24*(4), 623-640.

Center for Democracy & Technology. (2020). *Student data and information privacy: A survey of parents of K-12 students*. https://cdt.org/wp-content/uploads/2020/09/CDT-Parent-Student-Data-Privacy-Report-Slides.pdf

CESA 4. (2022). *Snapshot 2020-2021*. https://drive.google.com/file/d/1uVat68F3ftEIbEwM7FAAOhR88NIdpmxs/view

Children and Teens Online Privacy Protection Act, S. 748, 116th Cong. (2019). https://www.congress.gov/bill/116th-congress/senate-bill/748.

Costas, J., & Grey, C. (2014). Bringing secrecy into the open: Towards a theorization of the social processes of organizational secrecy. *Organization Studies*, *35*(10), 1423-1447.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed method approaches* (3rd ed.). Sage Publications.

Daggett, L. (2008). Student privacy and the Protection of Pupil Rights Act as amended by No Child Left Behind. *UC Davis Journal of Juvenile Law & Policy*, *12*(1), 51-132. https://heinonline.org/HOL/Page?handle=hein.journals/ucdajujlp12&id=53&collection=journals&index=#

Danzberger, J., Kirst, M., & Usdan, M. (1994). Governing the nation's schools: The case for restructuring local school boards. *Phi Delta Kappan*, *75*(4), 67-80.

Data Quality Campaign. (2020a). *Education data legislation review 2020*. Retrieved July 13, 2022 from https://dataqualitycampaign.org/resources/flagship-resources/education-data-legislation-review-20/

Data Quality Campaign. (2020b). *Maintaining trust as data use changes: Student data privacy and the COVID-19 crisis*. https://dataqualitycampaign.org/wp-content/uploads/2020/08/Student-Data-Privacy-and-COVID-19-08062020.pdf

Data Quality Campaign. (2021). *Education data legislation review 2021*. https://dataqualitycampaign.org/resources/flagship-resources/education-data-legislation-review-21/

Davies, R. S., & West, R. E. (2014). Technology integration in schools. In J. Spector, M. Merrill, J. Elen, & M. Bishop (Eds.), *Handbook of Research on Educational Communications and Technology* (pp. 841-853). Springer. https://doi.org/10.1007/978-1-4614-3185-5_68

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, *33*(3), 102-115. https://doi.org/10.1111/j.1540-4560.1977.tb01885.x

Dervarics, C., & O'Brien, E. (2019). Eight characteristics of effective school boards. *Center for public education*.

Dexter, S., & Richardson, J. W. (2020). What does technology integration research tell us about the leadership of technology? *Journal of Research on Technology in Education*, *52*(1), 17-36.

Dexter, S., Richardson, J. W., & Nash, J. B. (2017). Leadership for technology, use, integration, and innovation: A review of empirical research and implications for leadership preparation. In M. D. Young & G. M. Crow (Eds.), *Research on the Education of School Leaders* (2nd ed.). Routledge.

Electronic Privacy Information Center. (2016). Testimony of Caitriona Fitzgerald. In: Electronic Privacy Information Center.

Electronic Privacy Information Center. (2019). *Comments of the Electronic Privacy Information Center to the Federal Trade Commission: COPPA rule review* [Law revision recommendations]. https://epic.org/apa/comments/EPIC-FTC-COPPA-Dec2019.pdf

Electronic Privacy Information Center. (2022). *Data protection: Student privacy*. Retrieved 2022, July 17 from https://epic.org/issues/data-protection/student-privacy/

Fair, L. (2022, July 16, 2022). FTC to Ed Tech: Protecting kids' privacy is your responsibility. https://www.ftc.gov/business-guidance/blog/2022/05/ftc-ed-tech-protecting-kids-privacy-your-responsibility

Federal Trade Commission. (2012, December 19, 2012). *FTC strengthens kids' privacy, gives parents greater control over their information by amending Childrens Online Privacy Protection rule* https://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over

Federal Trade Commission. (2022). *Policy statement of the Federal Trade Commission on education technology and the Children's Online Privacy Protection Act*. ftc.gov Retrieved from https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection

Future of Privacy Forum. (2016). *Beyond one classroom: Parental support for technology and data use in schools*. https://fpf.org/wp-content/uploads/2016/12/Beyond-One-Classroom.pdf

Future of Privacy Forum. (2019). Policymaker's guide to student privacy. https://studentprivacycompass.org/wp-content/uploads/2019/04/FPF-Policymakers-Guide-to-Student-Privacy-Final.pdf

Future of Privacy Forum. (2020, November 24, 2020). *FPF and SIIA announce pledge 2020, an enhanced student privacy initiative* https://studentprivacypledge.org/news/pledge-2020-press-release/

Future of Privacy Forum. (2022, May 19, 2022). *FPF responds to the FTC's COPPA policy statement* [Press release]. https://studentprivacycompass.org/fpf-responds-to-the-ftcs-coppa-policy-statement/

Gahungu, A. (2018). Indiscipline and safety in public schools: Teachers and principals at odds. *International Journal of Research in Education and Science*, *4*(2), 375-390.

Glass, T. E., Bjork, L., & Brunner, C. C. (2000). *The Study of the American school superintendency, 2000. A look at the superintendent of education in the new millennium*. American Association of School Administrators. https://files.eric.ed.gov/fulltext/ED440475.pdf

Godkin, E. L. (1880). Libel and its legal remedy. *The Atlantic Monthly*, *46*, 729-738. https://www.unz.com/print/AtlanticMonthly-1880dec-00729/

Goodman, R. H. (1997). Getting there from here. School board-superintendent Collaboration: Creating a school governance team capable of raising student achievement.

Grant, D., Diliberti, M., Hunter, G., & Messan Setodji, C. (2020, December 15, 2020). *Remote learning here to stay despite challenges*. RAND Corporation. https://www.rand.org/news/press/2020/12/15.html

Greene, K. R. (1992). Models of school board policy making. *Educational Administration Quarterly*, *28*(2), 220-236. https://doi.org/10.1177/0013161X92028002004

Griswold v. Connecticut, 381 U.S. 479 (1965). https://supreme.justia.com/cases/federal/us/381/479/

Ham, M. J. (2021). *Big data in student data analytics: Higher education policy implications for student autonomy, privacy, equity, and educational value* (Publication Number 29262148) [Ph.D., The Ohio State University]. ProQuest Dissertations & Theses Global. Ann Arbor.

Hans, G. (2021). No exit: Ten years of "privacy vs. speech" post-Sorrell. *Wash. UJL & Pol'y*, *65*, 19.

Harris, A. (2020, april 4, 2020). Zoom banned from New York City schools due to privacy and security flaws. *Fast Company*. https://www.fastcompany.com/90486586/zoom-banned-from-new-york-city-schools-due-to-privacy-and-security-flaws

Hatch, J. A. (2002). *Doing qualitative research in education settings*. State University of New York Press.

Herold, B. (2017). COPPA and schools: The (other) federal student privacy law, explained. *Education Week*.

Hitt, D. H., & Tucker, P. D. (2016). Systematic review of key leader practices found to influence student achievement: A unified framework. *Review of Educational Research*, *86*(2), 531-569.

Hunt-Majer, C. (2022). Two bipartisan bills would protect kids and teens from instagram. *The Hill: Congress Blog*(July 16, 2022). https://thehill.com/opinion/congress-blog/two-bipartisan-bills-would-protect-kids-and-teens-from-instagram/

Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology, Research and Development*, *64*(5), 923-938. https://doi.org/https://doi.org/10.1007/s11423-016-9477-y

In re R.H., 791 A.2d 331 (Pa. 2002).

In re Tateana R., 883 N.Y.S.2d 476 (N.Y. App. Div. 2009).

International Society for Technology Education. (2022). *ISTE standards for education leaders*. International Society for Technology Education. Retrieved 5/3/2020 from https://www.iste.org/standards/for-education-leaders

Ishmael, K., Heiser, R., & Payne, J. (2020). *Pandemic planning for distance learning: Scenarios and considerations for PreK-12 education Leaders*.

https://www.newamerica.org/education-policy/reports/pandemic-planning-for-distance-learning-scenarios-and-considerations-for-prek12-education-leaders/

Ito, S. (2010, September 17). Pa. school district pays $33,000 to settle cell phone search lawsuit. *aclu.org*. https://www.aclu.org/blog/free-speech/student-speech-and-privacy/pa-school-district-pays-33000-settle-cell-phone-search

Jersey v. T.L.O., 469 U.S. 325 (1985). https://supreme.justia.com/cases/federal/us/469/325/

Johnson, A. (2019). So how much does it cost to educate a child in Wisconsin? *Milwaukee Journal Sentinel*. Retrieved 4/10/2020, from https://www.jsonline.com/story/news/2019/07/30/cost-educating-child-wisconsin-depends-where-you-live/1743930001/

Johnson, P. A. (2013). Effective board leadership: Factors associated with student achievement. *Journal of School Leadership*, *23*(3), 456-489. https://doi.org/10.1177/105268461302300302

Kids Online Safety Act, S. 3663, 117th Cong. (2022). https://www.congress.gov/bill/117th-congress/senate-bill/3663.

Kim, N. (2014). Three's a crowd: Towards contextual integrity in third-party data sharing notes. *Harvard Journal of Law and Technology*, *28*, 325.

Kingdon, J. W. (2003). *Agendas, alternatives, and public policies* (2nd ed.). Addison-Wesley Educational Publishers.

Kostick-Quenet, K. M., Cohen, I. G., Gerke, S., Lo, B., Antaki, J., Movahedi, F., Njah, H., Schoen, L., Estep, J. E., & Blumenthal-Barby, J. (2022). Mitigating racial bias in machine learning. *Journal of Law, Medicine & Ethics*, *50*(1), 92-100.

Krueger, K. R., & Moore, B. (2015). New technology "clouds" student data privacy. *Phi Delta Kappan*, *96*(5), 19-24.

Kshetri, N. (2020, November 6). Remote education is strife with threats to student privacy. *The Conversation*. https://theconversation.com/remote-education-is-rife-with-threats-to-student-privacy-148955

Kumar, P. C., Subramaniam, M., Vitak, J., Clegg, T. L., & Chetty, M. (2020). Strengthening children's privacy literacy through contextual integrity. *Media and Communication*, *8*(4), 175-184.

Land, D. (2002). Local school boards under review: Their role and effectiveness in relation to students' academic achievement. *Review of Educational Research*, *72*(2), 229-278.

LaRocque, L., & Coleman, P. (1993). The politics of excellence: Trustee leadership and school district ethos. *Alberta Journal of Educational Research*, *39*(4), 449-475. https://eric.ed.gov/?id=EJ478273

Lee, W. W., Zankl, W., & Chang, H. (2016). An ethical approach to data privacy protection. *ISACA Journal*, *6*. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection

Leithwood, K., Louis, K. S., Wahlstrom, K., Anderson, S., Mascall, B., & Gordon, M. (2010). How successful leadership influences student learning: The second installment of a longer story. In *Second International Handbook of Educational Change* (pp. 611-629). https://doi.org/10.1007/978-90-481-2660-6_35

Levin, B. B., & Schrum, L. (2012). *Leading technology-rich schools: Award-winning models for success*. Teachers College Press.

Levin, D. (2021). *The state of K-12 cybersecurity: 2020 year in review*. https://k12cybersecure.com/year-in-review/

Li, T. C. (2021). Post-pandemic privacy law. *American University Law Review*, *70*(5), 1681-1728.

Lim, S. M., Ghavifekr, S., & Kenayathulla, H. B. (2021). Optimizing the use of learning analytics through strategic direction and leadership practice: A higher education institution perspective. *MOJES: Malaysian Online Journal of Educational Sciences*, *9*(3), 25-36.

Markey, E., & Hatch, O. (2014, July 30). *Markey, Hatch introduce legislation to protect student privacy* https://www.markey.senate.gov/news/press-releases/markey-hatch-introduce-legislation-to-protect-student-privacy

Markey, E., & Hatch, O. (2015). Protecting student privacy in the digital age. *The Hill*(April 10, 2020). Retrieved May 15, from https://thehill.com/opinion/op-ed/241997-protecting-student-privacy-in-the-digital-age

Martin, K. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics*, *111*(4), 519-539. https://doi.org/10.1007/sl0551-012-1215-8

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, *137*(3), 551-569. https://doi.org/10.1007/s10551-015-2565-9

Marzano, R. J., Waters, T., & McNulty, B. A. (2005). *School leadership that works: From research to results*. Association for Supervision and Curriculum Development.

Maxwell, J. A. (2013). *Qualitative research design : an interactive approach* (3 edition. ed.). SAGE Publications, Inc.

McLeod, S., Bathon, J., & Richardson, J. W. (2011). Studies of technology usage are not enough: A response to the articles in this special issue. *Journal of Research on Leadership Education*, *6*(5), 288-297. https://doi.org/10.1177/194277511100600512

McLeod, S., Richardson, J. W., & Sauers, N. J. (2015). Leaching technology-rich school districts: Advice from tech-savvy superintendents. *Journal of Research on Leadership Education*, *10*(2), 104-126. https://doi.org/10.1177/1942775115584013

Mell, P., & Grance, T. (2010). The NIST definition of cloud computing [Article]. *Communications of the ACM*, *53*(6), 50-50.

Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation*. Jossey-Bass.

Molnar, A., & Boninger, F. (2015). *On the block: Student data and privacy in the digital age--The seventeenth annual report on schoolhouse commercializing trends, 2013-2014*. http://nepc.colorado.edu/publication/schoolhouse-commercialism-2014.

Mordecai, M. (2022). *Balancing student data privacy and innovation: Practices and perceptions in Hawai'i Public Schools* (Publication Number 29210448) [Ph.D., University of Hawai'i at Manoa]. ProQuest Dissertations & Theses Global. Ann Arbor.

N.N. v. Tunkhannock Area School District et al., 801 F. Supp. 2d 312 (M.D. Pa. 2011). https://dockets.justia.com/docket/pennsylvania/pamdce/3:2010cv01080/80867

National Association of Secondary School Principals. (2022). *Student data privacy*. https://www.nassp.org/top-issues-in-education/position-statements/student-data-privacy/

National Policy Board for Educational Administration. (2015). *Professional standards for educational leaders*. https://www.npbea.org/wp-content/uploads/2017/06/Professional-Standards-for-Educational-Leaders_2015.pdf

Neola. (2022). *Our process: Every district is unique*. https://neola.com/our-process/

Neola. (2023). *Administrative guidelines/procedures*. https://neola.com/services/

New Jersey v. T.L.O., 469 U.S. 325 (1985). https://supreme.justia.com/cases/federal/us/469/325/

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.

Nissenbaum, H. (2010). *Privacy in context*. Stanford Law Books.

Ohm, P. (2014). Changing the rules: General principles for data use and analysis. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 96-111). Cambridge University Press.

Ohm, P. (2015). Sensitive information. *Southern California Law Review*, *88*(5), 1125-1196. https://heinonline.org/HOL/P?h=hein.journals/scal88&i=1191

Owen, G. T. (2014). Qualitative methods in higher education policy analysis: Using interviews and document analysis. *The qualitative report*, *19*(26), 1.

Pandit, C., Kothari, H., & Neuman, C. (2020). *Privacy in time of a pandemic* 2020 13th CMI Conference on Cybersecurity and Privacy (CMI)-Digital Transformation-Potentials and Challenges (51275),

Pavesich v. New England Life Ins. Co., 122 Ga. 190 (Ga. 1905). https://casetext.com/case/pavesich-v-new-england-life-ins-co

Pepper, K. (2010). Effective principals skillfully balance leadership styles to facilitate student success: A focus for reauthorization of ESEA. *Planning and Changing*, *41*(1/2), 42-56. https://eric.ed.gov/?id=EJ952358

Prior, L. (2003). *Using documents in social research*. SAGE Publications. https://doi.org/10.4135/9780857020222

Prosser, W. (1960). Privacy. *California Law Review*, *8*, 388. https://www.jstor.org/stable/i276756

Protecting Student Privacy Act of 2014, S. 2690, 113th Cong. (2017). https://www.congress.gov/bill/113th-congress/senate-bill/2690.

Protecting Student Privacy Act of 2015, S. 1322, 114th Cong. (2015). https://www.congress.gov/bill/114th-congress/senate-bill/1322.

Protecting Student Privacy Act of 2017, S. 877, 115th Cong. (2017). https://www.congress.gov/bill/115th-congress/senate-bill/877.

Protecting the Information of our Vulnerable Children and Youth, H.R. 4801, 117th Cong. (2021). https://www.congress.gov/bill/117th-congress/house-bill/4801

Rachels, J. (1985). Why privacy is important. In D. G. Johnson & J. W. Snapper (Eds.), *Ethical Issues in the Use of Computers* (pp. 194-200). Wadsworth. http://public.callutheran.edu/~chenxi/Phil315_062.pdf

Rainsberger, R. (2018). The top 5 sections of the FERPA regulations: Understand legitimate educational interest. *The Successful Registrar*, *18*(1), 1-3.

Rammell, J. (2020). An uncertain balance: Student privacy rights in a dangerous world. *NML Rev.*, *50*, 223.

Raths, D. (2016). The patchwork of state student privacy laws [article]. *THE journal : technological horizons in education.* Retrieved April 24, 2020, from https://thejournal.com/articles/2016/10/13/the-patchwork-of-state-student-privacy-laws.aspx?admgarea=Features1&m=1

Reddy, A., & Vance, A. (2020). *Student privacy during the COVID-19 pandemic*. https://studentprivacycompass.org/wp-content/uploads/2020/03/COVID-19-Student-Privacy-FAQs-03-20-2020-1.pdf

Reidenberg, J., Russell, N. C., Kovnot, J., Norton, T., & Cloutier, R. (2013). Privacy and cloud computing in public schools. In *Center on Law and Information Policy* (Vol. 2).

Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education*, *16*(3), 263-279. https://doi.org/10.1177/1477878518805308

Richards, N. M., & Solove, D. J. (2010). Prosser's privacy law: A mixed legacy. *California Law Review*, *98*(6), 1887-1924. https://heinonline.org/HOL/P?h=hein.journals/calr98&i=1899

Richardson, J. W., Sauers, N. J., & McLeod, S. (2015). Technology leadership is just good leadership: Dispositions of tech savvy superintendents. *AASA Journal of Scholarship and Practice*, *12*(1), 11-30.

Richardson, J. W., & Sterrett, W. L. (2018). District technology then and now: A comparative study of district technology leadership from 2001 to 2014. *Educational Administration Quarterly*, *54*(4), 579-616.

Roche, D. (2020, September 2, 2020). *In continued rise more than 60% of U.S. K-12 public school students starting school virtually this fall* [Press Release]. https://www.prweb.com/releases/in_continued_rise_more_than_60_of_u_s_k_12_public_school_students_starting_school_virtually_this_fall/prweb17366345.htm

Rodríguez-Triana, M. J., Martínez-Monés, A., & Villagrá-Sobrino, S. (2016). Learning analytics in small-scale teacher-led innovations: Ethical and data privacy issues. *Journal of Learning Analytics*, *3*(1), 43-65.

Rodríguez-Triana, M. J., Prieto, L. P., Dimitriadis, Y., De Jong, T., & Gillet, D. (2021). ADA for IBL: Lessons learned in aligning learning design and analytics for inquiry-based learning orchestration. *Journal of Learning Analytics*, *8*, 22-50.

Roraback, C. G. (1989). Griswold v. Connecticut: A brief case history. *Ohio Northern University Law Review*, *16*, 395.

Rost, J. C. (1993). *Leadership for the twenty-first century*. Praeger.

Russell, N. C., Reidenberg, J., Martin, E., & Norton, T. B. (2019). Transparency and the marketplace for student data. *Virginia Journal of Law & Technology*, *22*(3), 107. https://heinonline.org/HOL/P?h=hein.journals/vjolt22&i=112

Russo, C. J. (2013). Fifth Amendment rights: Questioning students. *School Business Affairs*, *163*, 35-38.

Sabourin, J., Kosturko, L., FitzGerald, C., & McQuiggan, S. (2015). *Student privacy and educational data mining: Perspectives from industry* International Conference on Educational Data Mining,

Sallay, D., & Vance, A. (2020, March 27). *FAQs: The Protection of Pupil Rights Amendment*. FERPA Sherpa. Retrieved April 10, 2020 from https://ferpasherpa.org/faqs-ppra/

Sauers, N. J., Richardson, J. W., & McLeod, S. (2014). Technology-savvy school superintendents: Successes and challenges. *Journal of School Leadership*, *24*(6), 1177-1201.

Schwartz, P. M. (2013). The E.U. - U.S. privacy collision: A turn to institutions and procedures. *Harvard Law Review*, *126*(7), 1966-2009. https://heinonline.org/HOL/P?h=hein.journals/hlr126&i=2004

Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. *Calif. L. Rev.*, *102*, 877.

Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). Towards a standard for identifying and managing bias in artificial intelligence. *NIST Special Publication*, *1270*, 1-77.

Seashore Louis, K., Dretzke, B., & Wahlstrom, K. (2010). How does leadership affect student achievement? Results from a national US survey. *School Effectiveness and School Improvement 21*(3), 315-336.

Shaffer, G. (2021). Applying a contextual integrity framework to privacy policies for smart technologies. *Journal of Information Policy*, *11*, 222-265. https://doi.org/10.5325/jinfopoli.11.2021.0222

Shaw, T. (2014). Prioritizing the 21st century superintendent's skill set and knowledge base from the school board leadership perspective. In L. C. Kilmer, D. Halverson, R. Noppe, & B. Sheng (Eds.): ProQuest Dissertations Publishing.

Shen, F. X. (2013). Neuroscience, mental privacy, and the law: Privacy, security, and human dignity in the digital age. *Harv. J. L. & Pub. Pol'y*, *36*, 653.

Shu, C. (2020). *TikTok, WeChat and the growing digital divide between the US and China*. Tech Crunch. https://techcrunch.com/2020/09/22/tiktok-wechat-and-the-growing-digital-divide-between-the-u-s-and-china/

Skowronski, D. S. (2022). COPPA and educational technologies: The need for additional online privacy protections for students. *Georgia State University Law Review*, *38*(4), 12.

Slepian, M. L., Chun, J. S., & Mason, M. F. (2017). The experience of secrecy. *Journal of Personality and Social Psychology*, *113*(1), 1.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087-1155. https://doi.org/10.2307/3481326

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477-564.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Solove, D. J. (2016). A brief history of information privacy law. In K. J. Mathews (Ed.), *Proskauer on privacy: A guide to privacy and data security law* (2nd ed., pp. 1-51). Pracitising Law Institute.

Solove, D. J., & Schwartz, P. M. (2019). ALI data privacy: Overview and black letter text. *UCLA Law Review*, *68*, 46.

Sorrell v. IMS Health Inc., 564 U.S. 552 (2011). https://supreme.justia.com/cases/federal/us/564/552/

State v. Schloegel, 769 N.W.2d 130 (Wis. Ct. App. 2009).

Strickland, R. (2019). *The state student privacy report card* [privacy report card]. https://www.studentprivacymatters.org/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf

Student Privacy Compass. (2020a). *Education during a pandemic*. https://studentprivacycompass.org/resource/education-during-a-pandemic/

Student Privacy Compass. (2020b). *Education during a pandemic: Principles for student data privacy and equity*. https://studentprivacycompass.org/wp-content/uploads/2020/11/Education-During-a-Pandemic-Principles-2.pdf

Student Privacy Compass. (n.d.). *State student privacy laws*. Retrieved July 13, 2022 from https://studentprivacycompass.org/state-laws/

Takabi, H., Joshi, J. B., & Ahn, G.-J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24-31.

Talukder, S., Sakib, M., Islam, I., & Talukder, Z. (2020). Giving up privacy for security: A survey on privacy trade-off during pandemic emergency. *International Journal of Cryptography and Information Security (IJCIS)*, *10*(3). https://arxiv.org/abs/2007.04109

Tavani, H. T. (2008). Informational privacy: Concepts, theories, and controversies. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 131-164). John Wiley & Sons, Inc.

Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs*, *4*(4), 295-314. https://www.jstor.org/stable/pdf/2265075.pdf

Trainor, S. (2015). Student data privacy is cloudy today, clearer tomorrow. *kappanmagazine.org*, *96*(5), 13-18.

Trifiro, B. M. (2022). Breaking your boundaries: How TikTok use impacts privacy concerns among influencers. *Mass Communication and Society*, 1-24. https://doi.org/10.1080/15205436.2022.2149414

U.S. Department of Education. (2015). *Data security and management training: Best practice considerations*. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Security%20and%20Management%20Training_1.pdf

U.S. Department of Education. (2020a). *FERPA and the Coronavirus desease 2019 (COVID-19)*. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20Coronavirus%20Frequently%20Asked%20Questions.pdf

U.S. Department of Education. (2020b). *Protection of Pupil Rights Amendment (PPRA) General Guidance*. Retrieved June 28, 2022 from https://studentprivacy.ed.gov/resources/protection-pupil-rights-amendment-ppra-general-guidance

U.S. Department of Education. (2022a). *Personally identifiable information for education records*. https://studentprivacy.ed.gov/content/personally-identifiable-information-education-records

U.S. Department of Education. (2022b). *Who is a "school official" under FERPA?* . https://studentprivacy.ed.gov/faq/who-%E2%80%9Cschool-official%E2%80%9D-under-ferpa

U.S. Department of Education [USDOE]. (2022, March 1). *Family Education Rights and Privacy Act (FERPA)*. U.S. Department of Education. Retrieved 12/11/2022 from https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

U.S. Department of Health and Human Services. (2020a). *The HIPAA Privacy Rule*. U.S. Department of Health and Human Services. Retrieved 4/28/2020 from https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

U.S. Department of Health and Human Services. (2020b). *The security rule*. U.S. Department of Health and Human Services. Retrieved 4/28/2020 from https://www.hhs.gov/hipaa/for-professionals/security/index.html

United Nations Educational, S. a. C. O. (2022). *COVID-19 educational disruption and response*. Retrieved July 23, 2022 from https://webarchive.unesco.org/web/20200518115353/https://en.unesco.org/covid19/educationresponse/

van Leeuwen, A., Knoop-van Campen, C. A., Molenaar, I., & Rummel, N. (2021). How teacher characteristics relate to how teachers use dashboards: Results from two case studies in K-12. *Journal of Learning Analytics*, *8*(2), 6-21.

Vasalou, A., Joinson, A., & Houghton, D. (2015). Privacy as a fuzzy concept: A new conceptualization of privacy for practitioners. *Journal of the Association for Information Science and Technology*, *66*(5), 918-929. https://doi.org/10.1002/asi.23220

Venzke, C. (2022). *Federal policymakers should continue to build on recent steps to help K-12 schools secure their networks and protect student privacy*. Center for Democracy & Technology. Retrieved July 17, 2022 from https://cdt.org/insights/federal-policymakers-should-continue-to-build-on-recent-steps-to-help-k-12-schools-secure-their-networks-and-protect-student-privacy/

Vernonia School Dist. 47J v. Acton, 515 U.S. (1995). https://supreme.justia.com/cases/federal/us/515/646/

Wajnerman Paz, A. (2022). Is your neural data part of your mind? Exploring the conceptual basis of mental privacy. *Minds and Machines*, *32*(2), 395-415.

Wang, Y. (2016). Big opportunities and big concerns of big data in education [Article]. *TechTrends: Linking Research & Practice to Improve Learning*, *60*(4), 381-384. https://doi.org/10.1007/s11528-016-0072-1

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220. https://www.jstor.org/stable/pdf/1321160.pdf

Waters, J. T., & Marzano, R. J. (2006). *School district leadership that works: The effect of superintendent leadership on student achievement*. M.-c. R. f. E. a. Learning. https://files.eric.ed.gov/fulltext/ED494270.pdf

Waters, T., Marzano, R., & McNulty, B. (2003). Balanced leadership: What 30 years of research tells us about the effect of leadership on student achievement. *McREL*.

Weber, A. S. (2016). The big student big data grab. *International Journal of Information and Educational Technology*, *6*(1), 65-70. http://www.ijiet.org/vol6/660-DL1009.pdf

Webner, W. M. (1994). The right of publicity: A commercial property right - not a privacy right. *Trademark Reporter*, *84*, 586.

Welton, A. D., & Freelon, R. (2018). Community organizing as educational leadership: Lessons from Chicago on the politics of racial justice. *Journal of Research on Leadership Education*, *13*(1), 79-104.

Wesley, J. J. (2010). *Qualitative document analysis in political science* T2PP Workshop,

Westin, A. (1970). *Privacy and freedom*. The Bodley Head, Ltd.

Williams, R. D., & Center, P. T. C. (2020). Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security. *University of Pennsylvania: Philadelphia, PA, USA*.

Williamson, B., Eynon, R., & Potter, J. (2020). Pandemic politics, pedagogies and practices: digital technologies and distance education during the coronavirus emergency. *Learning, Media and Technology*, *45*(2), 107-114. https://doi.org/doi:10.1080/17439884.2020.1761641

Winter, J. S. (2012). Privacy and the emerging internet of things: using the framework of contextual integrity to inform policy. Pacific Telecommunciations Council Annual Conference Proceedings,

Wisconsin Department of Public Instruction. (2022a). *Student enrollment data* Wisconsin Department of Public Instruction. https://wisedash.dpi.wi.gov/Dashboard/dashboard/18110

Wisconsin Department of Public Instruction. (2022b). *Student records, part 1*. https://media.dpi.wi.gov/sspw/av/student-records-part-1/story.html

Wisconsin Legislative Council. (2017). *2016 legislative council study committee on school data*. Retrieved July 13, 2022 from https://docs.legis.wisconsin.gov/misc/lc/study/2016/1497/070_joint_legislative_council_recommendations_to_the_2017_18_legislature/jlcr_2017_01

Wisconsin State Legislature. (2018a). *Assembly Bill 71*. Retrieved July 13, 2022 from https://docs.legis.wisconsin.gov/2017/proposals/reg/asm/bill/ab71

Wisconsin State Legislature. (2018b). *Assembly Bill 72*. Retrieved July 13, 2022 from https://docs.legis.wisconsin.gov/2017/proposals/ab72

Wisconsin State Legislature. (2018c). *State of Wisconsin Senate Journal: One-hundred and Third Regular Session*. Retrieved July 13, 2022 from https://docs.legis.wisconsin.gov/2017/related/journals/senate/20180328/_9

Young, T., & Lewis, W. D. (2015). Educational policy implementation revisited. *Educational Policy*, *29*(1), 3-17. https://doi.org/10.1177/0895904815568936

VITA

Curtis C. Rees

Education

Southern Illinois University Edwardsville
Degree: Master of Arts
Major: Educational Administration

Augustana University, Sioux Falls, SD
Degree: Bachelor of Arts
Major: Elementary Education

University of Minnesota Morris
Degree: Bachelor of Arts
Major: Social Science; Focus in Political Science

Publications

Bathon, J., & Rees, C. C. (2023). Student records. In Decker, J. R., Lewis, M. M., Shaver, E. A., Blankenship, A. E., & Paige, M. A. *The Principal's Legal Handbook* (7th ed., forthcoming). Education Law Association.

Invited Presentations

Rees, C. C. (2015, December). *Design thinking in education*. Presentation at School Leaders Advancing Technology in Education.

Rees, C. C. (2015, December). *Student data privacy*. Presentation at School Leaders Advancing Technology in Education.

Rees, C. C. (2015, July). *Design thinking for education*. Presentation at K12 Learning Space Symposium.

Rees, C. C. (2015, July). *21st century learning spaces*. Presentation at K12 Learning Space Symposium.

Rees, C. C. (2015, February). *School culture*. Presentation at IntegratED Portland.

Rees, C. C. (2015, February). *21st century learning spaces*. Presentation at IntegratED Portland.

Rees, C. C. (2014, October). *School culture*. Presentation at IntegratED San Francisco.

Rees, C. C. (2014, October). *21st century learning spaces*. Presentation at IntegratED San Francisco.

Rees, C. C. (2013, December). *Don't fear the internet: Tech policies that keep kids safe and enhance learning*. Presentation at School Leaders Advancing Technology in Education.

Rees, C. C. (2012, October). *The connected administrator*. Presentation at the Association of Wisconsin School Administrators annual conference.

Rees, C. C. (2011, October). *Using Twitter to escape Administrator Island*. Presentation at the Association of Wisconsin School Administrators annual conference.

Rees, C. C. (2011, March). *Using the force of RtI & PLC*. Presentation at the Wisconsin RtI Summit.