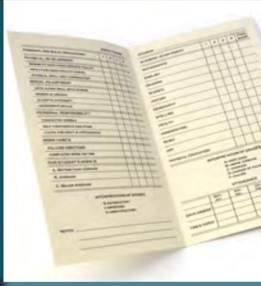
Forum Guide to Education Data Privacy



National
Forum
on Education
Statistics

Forum Guide to

Education Data Privacy

National Forum on Education Statistics

National Cooperative Education Statistics System

The National Center for Education Statistics (NCES) established the National Cooperative Education Statistics System (Cooperative System) to assist in producing and maintaining comparable and uniform information and data on early childhood, elementary, and secondary education. These data are intended to be useful for policymaking at the federal, state, and local levels.

The National Forum on Education Statistics (Forum) is an entity of the Cooperative System and, among its other activities, proposes principles of good practice to assist state and local education agencies in meeting this purpose. The Cooperative System and the Forum are supported in these endeavors by resources from NCES.

Publications of the Forum do not undergo the same formal review required for products of NCES. The information and opinions published here are those of the Forum and do not necessarily represent the policy or views of NCES or the U.S. Department of Education.

July 2016

This publication and other publications of the National Forum on Education Statistics may be found at the websites listed below.

The NCES Home Page address is *http://nces.ed.gov*
The NCES Publications and Products address is *http://nces.ed.gov/pubsearch*
The Forum Home Page address is *http://nces.ed.gov/forum*

This publication was prepared in part under Contract No. ED-CFO-10-A-0126/0002 with Quality Information Partners, Inc. Mention of trade names, commercial products, or organizations does not imply endorsement by the U.S. Government.

Suggested Citation
National Forum on Education Statistics. (2016). *Forum Guide to Education Data Privacy*. (NFES 2016-096). U.S. Department of Education. Washington, DC: National Center for Education Statistics.

Technical Contact
Ghedam Bairu
(202) 245–6644
ghedam.bairu@ed.gov

National Forum on Education Statistics

The work of the Forum is a key aspect of the National Cooperative Education Statistics System. The Cooperative System was established to produce and maintain, with the cooperation of the states, comparable and uniform education information and data that are useful for policymaking at the federal, state, and local levels. To assist in meeting this goal, the National Center for Education Statistics (NCES), within the U.S. Department of Education, established the Forum to improve the collection, reporting, and use of elementary and secondary education statistics. The Forum deals with issues in education data policy, sponsors innovations in data collection and reporting, and provides technical assistance to improve state and local data systems.

Development of Forum Products

Members of the Forum establish working groups to develop best practice guides in data-related areas of interest to federal, state, and local education agencies. They are assisted in this work by NCES, but the content comes from the collective experience of working group members who review all products iteratively throughout the development process. After the working group completes the content and reviews a document a final time, publications are subject to examination by members of the Forum standing committee that sponsors the project. Finally, Forum members (approximately 120 people) review and formally vote to approve all documents prior to publication. NCES provides final review and approval prior to online publication. The information and opinions published in Forum products do not necessarily represent the policies or views of the U.S. Department of Education or NCES.

Working Group Members

This online publication was developed through the National Cooperative Education Statistics System and funded by the National Center for Education Statistics of the U.S. Department of Education. The Education Data Privacy Working Group of the National Forum on Education Statistics is responsible for the content.

Co-Chairs

Dean Folkers, Nebraska Department of Education

David Weinberger, Yonkers Public Schools (New York)

Members

Dawn Gessel, Putnam County Schools (WV)

Laura Hansen, Metro Nashville Public Schools (TN)

Georgia Hughes-Webb, West Virginia Department of Education

Whitcomb Johnstone, Irving Independent School District (TX)

Marilyn King, Bozeman School District #7 (MT)

Julie Kochanek, Regional Educational Laboratory Midwest

Allen Miedema, Northshore School District (WA)

Steve Smith, Cambridge Public Schools (MA)

Michael Hawes, Privacy Technical Assistance Center, U.S. Department of Education

Consultant

Deborah Newby, Quality Information Partners

Project Officer

Ghedam Bairu, National Center for Education Statistics (NCES)

Acknowledgements

Members of the Education Data Privacy Working Group would like to thank everyone who reviewed or otherwise contributed to the development of the *Forum Guide to Education Data Privacy*. Many Forum members shared helpful insights from their states and districts, and the Forum's Policies, Programs and Implementation Committee provided constructive comments during the development of the document.

About This Guide

The National Forum on Education Statistics (Forum) organized the Education Data Privacy Working Group to explore how state and local education agencies (SEAs and LEAs) can support best practices at the school level to protect the confidentiality of student data in day-to-day instructional and administrative tasks. Many of the best practices applicable at the school level may also be helpful in protecting student data at the SEA and LEA levels. The Working Group created this guide in order to highlight common privacy issues related to the use of student data and present basic approaches to managing those issues. This document is not intended to serve as legal guidance, nor does it present a framework for a comprehensive privacy program. Many other excellent resources exist for those purposes. The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) offers legally authoritative resources on education data privacy. The information presented in this guide is based largely on the collective experience of the members of the Forum.

To illustrate the situations that occur in schools and education agencies, the Working Group developed a number of case studies. Each case study includes a description of the potential risk as well as various approaches that can be used to minimize the risk. The case studies are included in Chapter Two of the guide. In order to provide the necessary context for understanding the case studies, Chapter One of the guide presents an overview of important legal and procedural privacy concepts. The Appendices include references used in preparing the paper, additional resources, and sample privacy-related documents from districts.

Intended Audience

This guide was developed primarily as a resource for LEAs and SEAs to use in assisting school staff in protecting the confidentiality of student data. Education agencies may find the guide useful in developing privacy programs and related professional development programs.

Contents

Chapter 1: Overview of Education Data Privacy

The expanding use of student-level data and the dramatic upsurge in education technology tools are transforming public K12 education. Student-level data are being shared electronically not only across schools and districts within a state, but also with other agencies at both the state and local levels to improve services to students. Within the classroom, teachers are using student-level data in new ways to guide instruction and support team teaching. Student assessments—from pop quizzes to large-scale state tests—are frequently administered through computer-based applications. Homework assignments may now include the use of online apps or tutorials. While these trends in instructional practices are expanding opportunities for student learning, they are also bringing renewed attention to the importance of maintaining the confidentiality of student data and protecting student privacy. Best practices for the protection of student data must now encompass a variety of online platforms as well as electronic databases and traditional paper records.

The results of a 2015 Future of Privacy Forum (FPF) survey[1] showed that an overwhelming majority of parents support the use of student-level data by teachers and administrators within the school or school district for educational purposes, but they are significantly less comfortable with their schools sharing student data with online service providers or other third-party organizations.

In general, parental concerns about sharing student data with service providers include

- the potential use of student data for advertising or marketing purposes;
- the possible creation of individual student profiles by vendors, who may use the profiles for marketing purposes or sell the profiles to other entities;
- the risk of sensitive information about students—such as disciplinary or disability records—being shared online in ways that could impact a child's future educational or employment opportunities;
- the risk of identity theft; and
- other inappropriate uses of student data when the data are not properly protected or not properly deleted when no longer needed.

In addition to concerns related to the growth in educational technology and the expanding use of student-level data, the proliferation of wireless mobile devices and cloud-based technologies are causing concerns about the security of student data. The convenience, portability, and flexibility afforded by wireless devices and cloud-based services have had many positive impacts on the effective use of student data for improving education services, but the new devices and technologies have also created new concerns. Many staff use personal or district-owned mobile devices to store, analyze,

[1] The Future of Privacy Forum is a nonprofit organization that seeks to advance responsible data practices across various sectors, including education. https://fpf.org

and/or share student data. These devices may be more difficult to secure than traditional wired devices. Staff may also be using insecure methods for sharing student data with authorized staff or parents, such as sending the data via unprotected e-mail, or sharing files through insecure third-party, cloud-based storage services not approved by the agency.

The use of new technologies for instructional purposes holds great promise for personalizing education for students and facilitating instruction. However, education agencies need to responsibly balance instructional needs with privacy protections. This guide explores how state and local education agencies (SEAs and LEAs) can support best practices at the school level to protect the confidentiality of student data. The case studies found in Chapter Two highlight common student privacy issues and present various approaches to managing those issues. Chapter One provides the necessary context for understanding the case studies, and also presents information on how to implement formal privacy programs at the local level. There is no "one-size-fits-all" approach to protecting privacy. Education agencies need to consider state and federal laws, state and local school board policies, parental expectations, student instructional needs, and the agency's available resources when developing privacy guidelines and procedures.

This chapter presents an overview of

- the legal requirements that agencies must consider when developing privacy programs;
- the interrelationships of data governance, security, and privacy programs;
- considerations for effective staff professional development; and
- the roles and responsibilities of various entities in protecting the confidentiality of student data.

Privacy Laws

Education agencies[2] must consider all applicable federal and state laws when establishing privacy programs and procedures for protecting the confidentiality of student data. The most significant federal law governing the protection of student information is the Family Educational Rights and Privacy Act (FERPA), which sets forth the basic legal requirements for protecting student privacy. States may pass additional privacy laws that impose more stringent protections for student data, but state laws cannot weaken the requirements of FERPA. This section presents a general overview of FERPA and highlights other federal laws that are sometimes mentioned in discussions of education data privacy. It also provides examples of state laws that impose additional privacy requirements on education agencies within their respective states. **Please note that this section is not intended to be either an exhaustive or authoritative legal guide. All legal questions should be directed to the appropriate legal counsel within an education agency.**

Federal Privacy Laws

Family Educational Rights and Privacy Act (FERPA). FERPA sets forth the basic privacy requirements education agencies must meet, and serves as a foundation on which states and localities may build by adding more stringent privacy protections for student data. All schools that receive federal funds from a program administered by the Secretary of Education are subject to the requirements of FERPA. Originally passed in 1974, the law has been amended a number of times. In addition, the FERPA regulations were revised in 2008 and 2011. The regulatory revisions were prompted in large part by requests for clarification of the law by SEAs and LEAs, as well as the need to keep pace with changes in information technology. In order to assist education agencies, school officials, teachers, parents, and other education

[2] For the purpose of this document, "education agency" or "agency" refers to any entity which is covered by FERPA. This would include, but is not limited to, SEAs, regional educational agencies, LEAs, and schools.

stakeholders in understanding and implementing the requirements of FERPA, the U.S. Department of Education established the ***Privacy Technical Assistance Center (PTAC)***. PTAC offers a variety of resources related to student data and student data systems, including publications, training materials, and technical assistance. Resource topics include data privacy, confidentiality, and security practices.[3]

FERPA requires schools to give parents and eligible students (age 18 or older) the opportunity to review the information contained in a student's education records and request that any incorrect information be properly amended. In addition, FERPA generally prohibits schools from disclosing personally identifiable information (PII) from a student's education records to a third party without written consent from the parent or eligible student. Each school year, LEAs must notify parents and eligible students of their rights under FERPA.

The FERPA definition of PII includes direct student identifiers (e.g., name, student identification number, Social Security number), indirect identifiers (e.g., date of birth, address), and any other information that alone, or in combination with other information, is linked or linkable to a specific individual and would allow a reasonable person in the school community to identify the student (34CFR §99.3). Because this definition includes indirect identifiers and other linked or linkable information about the student, there is no definitive list of data elements considered to be PII under FERPA. Any student information may potentially be PII if it can be used by a reasonable person in the school community to identify the student. Aggregate or tabular data may be considered PII under FERPA if it includes information about individuals or small groups with unique or uncommon characteristics or extreme values. For more information about protecting aggregate data, see http://ptac.ed.gov/sites/default/files/FAQs_disclosure_avoidance.pdf.

Providing Information without Consent. FERPA allows a number of exceptions under which student PII may be shared without the consent of parents or eligible students. Four commonly used exceptions are briefly described below. It is important to note that under any of the exceptions, FERPA requires education agencies to use reasonable methods to ensure that any third party that receives student information uses the data only for authorized purposes and protects the data from future disclosures. In addition, under both the studies exception and the audit and evaluation exception, education agencies are required to ensure that the third parties destroy the data when the data are no longer needed for the purpose for which they were shared.

Under the **school official exception**, schools and LEAs may share student PII among designated school officials with a legitimate educational interest. Outside parties may be considered school officials if they are performing a service for which the school or LEA would otherwise use employees. LEAs define who constitutes a school official with legitimate educational interest in their annual notification of rights under FERPA.

The **studies exception** allows the disclosure of student PII to third parties that are conducting certain studies for, or on behalf of, educational agencies or institutions. These studies need to be for the specific (limited) purpose of developing, validating, or administering a predictive test, administering a student aid program, or improving instruction. Under FERPA, the education agency must first execute a written agreement with the organization conducting the activity. In general, FERPA requires that the written agreement

- specify the purpose, scope, and duration of the study and the information to be disclosed;
- require the organization to use PII from education records only to meet the purpose or purposes of the study as stated in the written agreement;

[3] For more information about PTAC, see http://ptac.ed.gov.

- require the organization to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than representatives of the organization with legitimate interests; and
- require the organization to destroy all PII from education records when the information is no longer needed for the purposes for which the study was conducted, as well as specify the time period in which the information must be destroyed.

The **audit or evaluation exception** allows the disclosure of student PII to authorized representatives of federal, state, and local educational authorities for the audit or evaluation of federal- or state-supported education programs. FERPA requirements for written agreements needed under the audit or evaluation exception are slightly different from those needed under the studies exception. The written agreement must

- designate the individual or entity as an authorized representative of the agency;
- specify the PII to be disclosed;
- specify that the purpose for which the information is being disclosed to the authorized representative is to carry out an audit or evaluation of federal- or state-supported education programs, or to enforce or to comply with federal legal requirements that relate to those programs;
- describe the activity with sufficient specificity to make clear that it falls within the audit or evaluation exception, including a description of how the information will be used;
- require the authorized representative to destroy the data when the information is no longer needed for the purpose specified and to stipulate how the data will be destroyed as well as the time period in which it will be destroyed; and
- require the authorized representative to establish policies and procedures to protect the PII from further disclosure and unauthorized use.

For more information about written agreements for sharing data under the studies exception and the audit or evaluation exception, see PTAC's *Guidance on Reasonable Methods and Written Agreements*, available at http://ptac.ed.gov/Guidance-Reasonable-Methods-Written-Agreements.

Under the **directory information exception**, schools may disclose certain student PII without the consent of the parent or eligible student. However, schools must first notify parents of the specific data elements the district is designating as directory information, and allow parents a reasonable amount of time to "opt out" of having their children's information shared under this exception. Schools must keep track of the children whose parents have opted out of sharing information, and ensure that information about these children is not included when directory information about other students is shared. The school district's directory information policy may be included as part of the requisite annual notification of FERPA rights, or it may be distributed separately.

Directory information can be defined as PII that is generally not considered harmful or an invasion of privacy if released. LEAs are responsible for developing the directory information policy that will be used in their schools. The list of data elements considered to be directory information will vary among LEAs. Some SEAs may establish a minimum directory information policy. LEAs in states with a minimum directory information policy must include all of the data elements in the SEA policy as part of the LEA's directory information policy.

Directory information may include the following student information:

- Name
- Address
- Telephone listing
- Electronic mail address
- Photograph
- Date and place of birth
- Major field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received
- The most recent education agency or institution attended

Districts typically use directory information for school-related purposes, such as the following:

- A playbill or other program showing student roles in drama or music productions
- Sports activity sheets
- Yearbooks
- Honor rolls or other recognition lists
- Graduation programs

In addition, schools may share directory information with outside organizations, such as companies that manufacture class rings.

It is important to note that when designated directory information is combined with any other information about the student that is NOT considered directory information, the directory information exception does not apply. For example, a list that includes student names, addresses, and telephone numbers would fall under the directory information exception if those three data elements are designated as directory information. But if the list also includes each student's ethnicity, the list would no longer be eligible for sharing under the directory information exception.

Some districts may choose to adopt a limited directory information policy. Under this type of policy, an LEA can either (a) designate the specific entities that may receive directory information, or (b) designate the specific purposes for which directory information may be shared. Parents and eligible students must still be notified of the directory information policy and allowed to opt out. Some districts may decide to adopt such a policy because it gives them better control over which organizations can have access to the data. In particular, schools and districts in states or localities that have open record laws may find it difficult to refuse to share directory information with an external organization unless the district has specifically adopted a limited directory information policy.

Other FERPA exceptions exist that allow for sharing student data with

- officials at another school to which a student is transferring, even if the new school is in a different state;
- law enforcement or court officials in compliance with a judicial order or subpoena;
- appropriate officials in cases of health and safety emergencies;
- case workers for children in foster care or who are wards of the state; and
- state and local officials within a juvenile justice system, in accordance with state law.

For more detailed information on the FERPA exceptions, see the *FERPA Exceptions Summary* at http://ptac.ed.gov/sites/default/files/FERPA%20Exceptions_HANDOUT_horizontal_0.pdf.

Explaining Personally Identifiable Information to Education Stakeholders

The following description was developed by the West Virginia Department of Education to help educators and other stakeholders, including the public, understand personally identifiable information (PII).

Personally identifiable information (referred to as "PII") includes any information that can be used, either alone or in combination with other information, to directly determine or find the identity of an individual person. PII can include a person's name, Social Security number (SSN), other individual identification number (such as WVEIS[a] identifier for students), address, and so on. It can also include distinct pieces of information that, when combined, can identify an individual. In the case of student education records, that might include a student's grade level, date of birth, and/or other personal information (e.g., gender, race, or ethnicity). PII stored in students' education records is protected by federal and state law.

Although all PII is protected, some PII is considered sensitive information because if it is lost, exposed to unauthorized parties, or misused, there could be an adverse impact for the individual. The combination of two or more pieces of non-sensitive PII may result in sensitive information, as when a person's full name is associated with their date of birth and mother's maiden name—information often used to verify a person's identity for credit purposes. Both the potential for harm and the context in which the information is used are important determinants of what constitutes "sensitive" PII. For instance, a list of students attending a particular school may include PII (students' names) but would not be considered sensitive, given that revealing only student names would not likely result in harm to the individual students. A list of students receiving specific services at the school, such as academic tutoring or counseling, would be considered sensitive, given that exposing such information may open those student to harm such as ridicule from their peers or others based on the nature of the services they receive.

[a] WVEIS stands for West Virginia Education Information System, the state's centralized longitudinal data system used by all districts for administrative record keeping and reporting.

Protection of Pupil Rights Amendment (PPRA). Personal information collected directly from students and student surveys on certain sensitive topics may be subject to the specific requirements and provisions of PPRA. This law requires that schools allow parents to see any instructional or survey materials that will be used with their children, and it requires parental consent before minor students can participate in a survey administered by the U.S. Department of Education that reveals certain types of information including, but not limited to, political affiliations, mental health, sexual behavior and attitudes, illegal behaviors, or income.

Individuals with Disabilities in Education Act (IDEA). IDEA is the federal law designed to protect students with disabilities and ensure they receive equitable treatment. It also includes specific provisions addressing student privacy. In general, FERPA requirements apply under IDEA. One difference, however, is that under IDEA when a child with disabilities reaches the age of 18 and becomes an "eligible" student under FERPA, an education agency must continue to send notifications to the parents in addition to the eligible student.

Children's Online Privacy Protection Act (COPPA). Administered and enforced by the Federal Trade Commission, COPPA protects children under the age of 13 who use commercial websites, online games, and mobile applications. The vendor responsible for the websites, games, or applications is responsible for meeting the privacy requirements of COPPA. While LEAs certainly have an obligation to take steps to make sure the services their students use treat the data they collect responsibly, COPPA ultimately puts requirements for adherence on the online service operator. The law generally does not apply to websites maintained by education agencies, other government agencies, or nonprofit organizations, nor does it usually apply where an education agency has contracted with a website operator to collect information from children for educational purposes for use by the education agency. In those instances, the education agency (not an individual teacher) can provide consent on behalf of the students when it is required as long as the data are used only for education purposes. If a vendor wants to use data for other purposes, parental consent is needed. Although COPPA may not always apply in educational settings, education agencies may find it helpful to remind vendors of COPPA requirements as a way to emphasize the vendor's responsibilities in protecting student privacy.

Enacted in 1998 and implemented in 2000, COPPA requires operators of commercial websites or online services directed to children under 13 to

- post an online privacy policy that describes the company's information practices for personal information collected online from children;
- provide direct notice to parents and obtain verifiable parental consent (with limited exceptions) before collecting personal information online from children;
- give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties;
- provide parents access to their child's personal information to review and/or request that the information be deleted, and/or prohibit future use or collection of data;
- maintain the confidentiality, security, and integrity of information they collect from children; and
- delete the child's information once the purpose for which it was collected has been fulfilled.

COPPA defines "personal information" as a child's

- first and last name;
- home or other physical address, including street name and city or town;
- online contact information;
- a screen name or user name that functions as online contact information;
- telephone number;
- Social Security number;
- a persistent identifier that can be used to recognize a user over time and across different websites or online services;
- a photograph, video, or audio file, where such file contains a child's image or voice;

- geolocation information sufficient to identify a street name and name of a city or town; and
- information concerning the child or the child's parents that the operator collects online from the child and combines with an identifier described above (FTC 2015).

Health Insurance Portability and Accountability Act (HIPAA). In addition to making it easier for individuals to keep their health insurance, HIPPA also protects the confidentiality and security of healthcare information. Although HIPAA is frequently mentioned in discussions about federal privacy laws, it is important to note that information considered to be part of an education record under FERPA is not subject to HIPAA requirements. Thus, HIPAA rarely applies to K12 schools because most schools either are not HIPAA-covered entities, or they are HIPAA-covered entities but maintain health information on students only in records that are by definition education records under FERPA. For more information, see the U.S. Department of Education's Family Policy and Compliance Office's *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records*, available at http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf.

National School Lunch Act (NSLA). The NSLA created the National School Lunch Program to provide low-cost or free meals to qualified students. Student eligibility for free- or reduced-price lunch (FRL) is determined primarily by a student's family income. NSLA governs the disclosures of information about a student's FRL status. If a student's FRL eligibility status or the income information collected in order to determine the status is maintained as part of the student's education record, FERPA disclosure rules apply in addition to NSLA guidelines. For more information about permitted disclosures of FRL data, see Chapter 5: Confidentiality and Disclosure of the 2015 edition of the *Eligibility Manual for School Meals. Determining and Verifying Eligibility*, published by the U.S. Department of Agriculture, Food and Nutrition Service. http://www.fns.usda.gov/sites/default/files/cn/SP40_CACFP18_SFSP20-2015a.pdf.

Military Recruiters. In 2001 and 2002, Congress passed two pieces of legislation concerning military recruiters' access to student information: the No Child Left Behind Act of 2001 and the National Defense Authorization Act for Fiscal Year 2002. These laws generally require LEAs that receive assistance under the Elementary and Secondary Education Act (ESEA) to give military recruiters the same access to secondary school students as they provide to postsecondary institutions or to prospective employers, and to provide students' names, addresses, and telephone listings to military recruiters when requested. FERPA's directory information exception applies to information requests from military recruiters, so the information cannot be supplied if a parent has opted out of sharing directory information.

Examples of State Privacy Laws

Oklahoma's Student Data Accessibility, Transparency, and Accountability Act (Student DATA Act) of 2013 included a number of provisions designed to restrict the use of student-level data and improve transparency with the public about how the data are used. Among these provisions, the SEA was required to

- publicly post an inventory of the types of student data collected by the agency;
- develop policies regarding who can access student data;
- limit the sharing of student data with entities outside of Oklahoma;
- develop a security plan and conduct regular security audits of the state's data system; and
- include language in contracts with vendors (including online service providers) to guarantee adherence to privacy and security provisions of state and federal law.

The Oklahoma Student Data Act was used as model legislation by a number of other states, including **West Virginia**. The Student Data Accessibility, Transparency, and Accountability Act was passed by the West Virginia legislature in 2014. It includes similar requirements to the Oklahoma statute and also mandates the establishment of a formal privacy program and prevents the collection of certain types of student data.

Louisiana passed two laws concerning the protection of student data. R.S. 17:3914, **Act 837 of 2014**, prohibits LEAs from sharing students' PII, including students' names, Social Security numbers, dates of birth, and addresses, unless the data sharing meets one of the law's limited exceptions. For any data sharing not explicitly allowed for under the law, LEAs must first obtain written consent from parents. The law also requires local school boards that contract with private entities to ensure the privacy of students' personal information through contractual requirements, including breach planning and remediation procedures. In addition, the law required the SEA to discontinue its use of student Social Security numbers as statewide student identifiers and develop anonymous student identifiers. Under this law, unlawful disclosure of personally identifiable student information is punishable by a fine of not more than ten thousand dollars or imprisonment for not more than three years, or both. R.S. 17:3913, **Act 677 of 2014**, requires that Louisiana's SEA and LEAs make available information about the transfer of students' PII.

California's Student Online Personal Information Protection Act (SOPIPA) was passed in 2014. This law is considered by many to be a landmark state law by shifting the responsibility for appropriate data use from the education agency to the vendors with whom the agency does business (CCSSO 2014). SOPIPA prohibits an operator of an Internet website, online service, online application, or mobile application from knowingly engaging in targeted advertising to students or their parents; creating, maintaining, or sharing student profiles for non-educational purposes; or selling or disclosing student data except under limited circumstances. In addition, online service providers are required to maintain reasonable security procedures and delete student information at the request of the school or district that has contracted for services with the vendor. Service providers are allowed to use de-identified student data for the "development and improvement of educational sites, services, or applications" (CLI 2014). A number of states subsequently passed laws based on California's SOPIPA. In addition, the federal Student Digital Privacy Act that was introduced in the House in April 2015 was based largely on California's SOPIPA.

Fifteen additional states passed new student data privacy laws in 2015. Some of the new state laws focused on the responsibilities of education agencies in protecting student privacy. For example, **North Dakota** passed S**enate Bill No. 2326**, which specifically requires every local school board in the state to adopt a policy regarding the protection of student data. These policies must require that permission be obtained from the school board before any student data are shared with an individual who is not a school district employee (or the student's parent), or shared with any other entity. In addition, the school board policies must require the school district superintendent to compile a list of all individuals with whom, and entities with which, student data are shared; and a list, by title, of all school district personnel who have access to student data.

Other state laws passed in 2015 address the responsibilities of online service providers, similar to California's SOPIPA. For example, **Washington** passed the **Student User Privacy in Education Rights Act (SUPER)**, which addresses the obligations of school service providers with regard to transparency, choice and control, and safeguards.

Interrelationships of Data Governance, Data Security, and Privacy

Privacy programs are often implemented in conjunction with an agency's data governance program, which encompasses all the processes, rules, and systems relating to the quality, collection, management, and protection of student data. Both privacy and security considerations are needed for the protection of student data. Although closely related, privacy and security are slightly different. Privacy policies and procedures are usually focused on adhering to the legal and ethical requirements for protecting the confidentiality of data. These requirements involve defining which data need to be protected (such as PII or sensitive data), developing policies that define acceptable uses for the data, identifying authorized users of the data, protecting data that are released in public reports, and destroying data when they are no longer needed. Security policies and procedures focus on technical aspects of protecting the data within the information technology infrastructure and user applications and tools. Agencies without a data governance program may want to consider establishing data privacy and security programs. All three types of programs can be designed to address the various phases of the information lifecycle. This section summarizes the information lifecycle, reviews the basic considerations for a comprehensive data governance system, and discusses specific components of stand-alone privacy and security programs.

Information Lifecycle

Information has a lifecycle that begins with defining data needs and ends with destroying the data when they are no longer needed. The basic stages of the information lifecycle are described below (NFES 2010).

- **Define**. Before collecting data, education agencies need to identify and define the data elements they need in order to comply with reporting requirements or to inform decisionmaking and business processes. Only data that are needed for a legitimate purpose should be collected.
- **Collect**. Some information will need to be collected only once. After it is collected and entered into a student information system, it is likely to remain constant over time. Examples of this type of information include a student's name and birth date. Other data are the products of recurring events or activities, such as course enrollments, program participation, testing, and so on. These data need to be collected on a regular basis.
- **Store and Protect**. Education data are stored in various ways. At the state level, student data may be stored in a statewide longitudinal data system. In some instances, the SEA stores student data for its LEAs as well. In most cases, LEAs are responsible for storing student data in a data system that is owned and operated by the LEA. Regardless of where the data are stored, the agency responsible for the data system that houses the data bears primary responsibility for the security of the data. Protection of the data involves both security and privacy considerations, including defining user roles and access rights.
- **Use**. The most important part of the data lifecycle is the use of the data. Effective data systems facilitate the use of the data to support the organization's work and the students' educational outcomes. Authorized users will need a variety of tools to access and analyze the data.
- **Share**. Policies on how, when, under what circumstances, and with whom (individuals, organizations, other systems) the data will be shared are subject to privacy laws and regulations. In addition, when data are released to the public, steps must be taken to protect the privacy of individual students.
- **Retire**. One of the last decisions to be made in the data lifecycle comes when specific data are no longer needed for the purposes for which they were originally collected and stored. Some data, such as transcript data, may need to be properly secured and archived in case they are needed in the future. Other data should be destroyed once they are no longer needed for any authorized purpose.

Data Governance

In general, data governance refers to the overall management of the availability, usability, integrity, quality, and security of data (NCES 2012). By clearly outlining policies, standard procedures, responsibilities, and controls surrounding data activities at each point in the data lifecycle, a data governance program helps to ensure that information is collected, maintained, used, and disseminated in a way that protects individuals' rights to privacy, confidentiality, and security, while producing timely and accurate data. A comprehensive data governance structure will include both privacy and security policies and procedures.

Data governance councils (or committees or programs) were adopted in most SEAs as the agencies were building their statewide longitudinal data systems. The growing amount of individual student data collected and stored electronically by education agencies led to greater scrutiny of data management and protection practices. Data governance programs help ensure that appropriate policies and procedures are in place to facilitate access to and use of student data while protecting student privacy. Some LEAs have also adopted data governance programs as their use of data continues to expand.

At the state level, there may be both a K12 and a P20W data governance system. The K12 data governance system manages issues related to the data maintained in the SEA student data system. The P20W data governance system manages issues related to sharing data on individual students from preschool through the workforce that are housed in multiple data systems managed by multiple state agencies. The P20W data governance system must deal with varying security requirements, data uses, reporting schedules, and data dictionaries. At the LEA level, data governance is typically focused on student K12 education data. However, with the growth in community-based schools and the associated sharing of data among various non-profit agencies in the locality, some LEAs may find a cross-agency data governance structure to be helpful.

A data governance structure generally has various levels of responsibility and decisionmaking. An example of a data governance structure with four levels of responsibility is described below (NCES 2012).

- Level 1. The Information Technology Department is responsible for the infrastructure that collects, stores, reports, and manages access to the data within the data system. It is also typically responsible for managing the technical security of the data.
- Level 2. The Data Stewards or Managers who represent the various program areas that use student data meet regularly to discuss issues related to which data are needed and how they are used. The individuals in this group would be representatives from program offices within the agency, such as Special Education, Career and Technical Education, Migrant Education, and so on. In addition, school support staff are often the experts on directory information and other student data, and they can provide important perspectives on how those data are used.
- Level 3. The Data Management Committee is responsible for coordinating activities among the data stewards, the IT staff, and other stakeholders. It would also include representatives from either LEAs (at the SEA level) or school buildings (at the LEA level).
- Level 4. The Data Policy Committee is responsible for setting key policies for the agency and carrying out the legal and policy directives of the agency's leadership. At the SEA level, these might include senior staff from the agency along with representatives from the governor's office and other partnering state agencies

or entities. At the LEA level, these might include representatives from the local school board office as well as senior administrative staff within the district. Cross-agency data governance committees would include representatives from all agencies at each level of responsibility and decisionmaking.

Another example for effective data governance outlines typical areas of responsibility for data governance councils, as listed below (PTAC 2015-a, PTAC 2015-b). Across each of these areas, the data governance council would be responsible for assigning roles and responsibilities to each level of decisionmaking described above.

- **Data inventory**. Maintaining a complete up-to-date inventory of all data that are collected as well as all data systems—including those used to store and process data—enables the agency to target its data security and privacy management efforts to appropriately protect PII and sensitive data.
- **Data quality**. Identifying strategies for preventing, detecting, and correcting errors and misuses of data is essential to maintaining high-quality data.
- **Data use and access**. Good data management requires specifying all approved uses for the data as well as all authorized users of specific data.
- **Data sharing and reporting**. Ensuring that data dissemination activities comply with federal, state, and local laws is a key responsibility of a data governance council. The release or sharing of any data without written consent (e.g., in the form of individual records or aggregate reports) must adhere to the policies and regulations established by the organization, including procedures for protecting PII when sharing with other agencies and disclosure avoidance procedures for protecting PII from disclosure in public reports. In addition, the data governance plan will typically specify procedures for regular stakeholder notification about their rights under federal, state, and local laws governing data privacy.
- **Data security and risk management**. Ensuring the security of student PII and sensitive data by defending against the risks of unauthorized disclosure is a top priority for an effective data governance program.

Data Security

The term "data security" refers to protecting the technical aspects of how data are collected, stored, and transferred through an information technology infrastructure. The infrastructure may include agency-owned servers and devices—including mobile devices—as well as agency-controlled applications, networks, and cloud-based storage devices. At one time there may have been a relatively clear divide between internal and external security threats, with a firewall serving as the divide, but this is no longer always the case. The extensive use of mobile devices by staff—both agency-owned and personal devices—along with the growing use of online applications in the classroom that are not hosted or maintained by the agency are making it more challenging for agencies to anticipate and manage potential security risks.

Protecting Paper Records

Although data privacy discussions are generally focused on electronic data, it is important to remember that data stored in paper records must also be protected from misuse and unauthorized access. Data contained in paper records may only be shared in accordance with federal, state, and local laws and policies. Paper records must be securely maintained and disposed of properly when no longer needed, according to the agency's records retention policy.

Although the line between internal and external threats is blurring, there remains the division between technical threats or risks (e.g., an outsider hacks into a database that was not properly secured) and human risks (e.g., someone leaves his password by his computer). A comprehensive data security management plan will help reduce both kinds of risks. A good plan will include policies and guidelines that specify rules for work-related and personal use of all organizational computer and data systems, as well as the business use of all personally owned devices. The plan will also include policies and procedures for data use, assessing data risks, and handling data security breaches, as well as an explanation of how compliance with these policies is monitored. ***Staff professional development is essential to the success of security programs***. It is critical to conduct regular staff trainings and compliance audits to ensure that organizational policies and procedures are understood and followed. An agency may have the best technical safeguards in place, but if staff are not properly trained the processes will fall apart.

Protecting Against Technical and Human Threats

Listed below are examples of how an agency can guard against security threats (PTAC 2015-c).

- **Physical security**. Make sure computing resources are physically unavailable to unauthorized users. This includes securing access to any areas where PII or sensitive data are stored and processed, such as buildings and server rooms. Monitor access to these areas to prevent intrusions. Require ID badges and/or visitor log-ins prior to entering the secure areas or using the equipment.
- **Network security**. A network map can provide a critical understanding of the network and its connections (including servers, routers, applications, and associated data). A good network map will show the dependencies between applications, data, and network layers, and highlight potential vulnerabilities. Use firewalls and intrusion detection/prevention systems. A firewall is a device designed to permit or deny network transmissions based upon a set of rules. Intrusion detection and prevention systems can help detect and prevent malicious activity on the network.
- **Secure configurations**. New hardware or software should not be added to a network until it has been security tested and configured to optimize security. Inaccurate configurations or sharing permissions can unintentionally leave personal information open to web searching and browsing.
- **Patch management**. A patch is a piece of code that protects computers and applications by updating the security features to protect against new threats or vulnerabilities. Patches should be applied as part of a comprehensive plan for regular system testing and rollouts of software updates and patches.
- **Two-factor authentication**. Authorized users can be authenticated (identified) through the use of passwords, key cards or tokens, or biometrics (such as fingerprints). Two-factor authentication requires the simultaneous use of two of these methods.
- **Access control**. Securing data access includes requiring strong passwords and multiple levels of user authentication, setting limits on the length of data access (i.e., locking devices after they have been idle for a set period of time), limiting access to sensitive data and resources to those with a need to know, and limiting administrative privileges. It is important for agencies to have policies in place to ensure that separated employees no longer have access to data.
- **Encryption of data**. Sensitive data stored on servers or mobile devices, such as laptops or smart phones, should be encrypted. This limits the probability that sensitive data can be retrieved from the device if it is lost or stolen. In addition, sensitive data should be encrypted or de-sensitized before they are transmitted via e-mail.
- **Staff security training**. Staff training is the most important component of a good security program. Outlined below are some of the security issues that are problematic among staff in many agencies. In the event that an unauthorized user may have gained access to student data through staff negligence related to one of the issues discussed here, staff are responsible for notifying appropriate school or district officials of a potential

data breach. PTAC offers districts customizable training materials on responding to data breaches at http://ptac.ed.gov/document/data-breach-response-training-kit.

- Password Management. It is important for staff to be trained on developing effective passwords and changing passwords periodically. Some systems automatically require complex passwords and periodic changing. Encourage staff to use Post-it notes to remind others in the school when they notice a security lapse. For example, if Ms. Jones notices that Ms. Smith has left her password information out near her computer, Ms. Jones can remove the password information to a more secure location and leave a note for Ms. Smith as to where she can find it. That brings immediate attention to the issue on a personal level.
- Locking Computers. Most school districts are able to automatically force lockdown of a staff person's computer after it has been sitting idle for a certain amount of time. There is still a danger, however, that students can quickly access a teacher's computer the minute a teacher has stepped out of the room. Teachers should be reminded to lock their computers if they need to step away, particularly while students are present.
- Sending Sensitive Student Data Via Email. There are times when it is necessary for agency staff to send student data via e-mail to an authorized school official. For example, a district may want to confirm that a student has successfully enrolled in the state's virtual school and is making progress. The easiest option is to send the request, with only the student's statewide identifier, to the virtual school for confirmation. Some districts use encrypted e-mails sent through the district's e-mail server. In general, external, unencrypted e-mail should never be used to discuss student-level data. In some circumstances, communication with others outside the firewall and in otherwise unsecure exchange is with a password-protected spreadsheet with a separate communication of the password.
- Using Personal Mobile Devices. Some agency staff choose to use their personal mobile devices to store or send student data. Although some agencies have found ways to segment personal devices so that school data are in an area of the device controlled by the district, not all agencies can ensure the security of these devices or back up the data on the devices. An important consideration for staff in using personal mobile devices for business is that personal devices can be subpoenaed if required under legal discovery proceedings, meaning that personal data may be revealed. Staff who use personal devices for business must understand the importance of using a password on the device in order to protect the data. One quick way to remind individuals of the importance of password-protecting their devices if they are using them for official business is to ask people in a workshop to pass their phones to someone else. It's easy to see who has their phone password-protected.
- Data Destruction. A best practice for maintaining the confidentiality of student data is to delete the data from electronic storage devices when the data are no longer needed. For paper-based data, the solutions are to shred or burn the paper. (Note that any decision to burn paper records should be made in accordance with local air quality regulations.) For electronic devices, simply deleting a file may be insufficient. There are three general methods of data destruction to help prevent the possibility of data recovery after a file has been deleted: clear, purge, or destroy. Clearing data involves applying programmatic techniques to protect against the possibility of data recovery, typically applied through the standard read and write commands such as rewriting with a new value or using a menu option to reset the device to the factory state. In addition, there are a number of commercial products available that will delete files so they are not recoverable. Purging involves applying physical or logical techniques that completely eliminate the data on the device, and destroying involves destroying the data storage device

so that it cannot be reused. For more information, see PTAC's Best Practices for Data Destruction, available at http://ptac.ed.gov/document/best-practices-data-destruction.

- Phishing. An important topic to discuss in security training is phishing, a form of social engineering. Social engineering can be defined as the practice of extracting confidential information from people through false pretenses. According to the Federal Trade Commission, "when internet fraudsters impersonate a business to trick you into giving out your personal information, it's called phishing. Don't reply to e-mail, text, or pop-up messages that ask for your personal or financial information. Don't click on links within them either – even if the message seems to be from an organization you trust. It isn't. Legitimate businesses don't ask you to send sensitive information through insecure channels" (FTC 2016).

  It is still not uncommon for school staff to inappropriately respond to phishing attempts to gain student information or to gain staff log-in information to computer systems. Staff need to understand how to evaluate such requests for authenticity and appropriately respond.

Privacy Programs

A good privacy program considers all legal and ethical requirements in defining PII and sensitive data, deciding which PII or sensitive student data can be collected, identifying staff members who need access to the data for specific uses, and following appropriate procedures for safely and legally disclosing data. In addition, a strong security program is essential in supporting a privacy program.

PTAC offers a video and companion checklist for districts on the topic of developing a privacy program (PTAC 2015-d). These resources define a privacy program as a set of policies and procedures designed to help districts keep student personal information safe, comply with privacy law, and protect students and districts from harm. Once the agency's leadership determines that a privacy program is needed, key steps in establishing the program include the actions listed below.

- ✓ Designate a staff person to serve as the privacy coordinator. That individual's official job requirements should include responsibility for coordinating privacy efforts and policies.
- ✓ Work with the agency's data governance council (if one exists) or legal staff to determine which privacy policies and procedures are already in place.
- ✓ Bring the right people to the table to determine which policies and procedures are needed at each phase of the data lifecycle. For example, agency data managers, IT staff, school administrators, and instructional staff may be helpful in developing and implementing the program.
- ✓ Train all data users on privacy policies and procedures.
- ✓ Implement a monitoring plan to ensure that policies and procedures are being followed.
- ✓ Communicate with parents about the agency's efforts to protect student privacy.

An agency privacy program helps protect students and the district from potential harm by meeting legal and ethical requirements for protecting PII in student education records. A good privacy program protects student PII at each point of the education data lifecycle.

Transparency

Many new state privacy laws require education agencies to provide information to the public about the student data collected by the agency. Thus, transparency has become an important consideration for both SEAs and LEAs. Agencies may be required to provide data inventories listing all data collected by the agency. The required level of specificity varies. Some agencies may need to provide complete lists of all data elements; others may need to provide only general categories of data. In addition, agencies may be required to provide information on how the data are used and how the agency protects the confidentiality of the data.

Some suggested practices for maximizing transparency with the public include

- making information about student data policies and practices easy to find on the district's public webpage;
- publishing a data inventory that details the student information collected by the district and explains how it is used;
- posting contracts online, including terms of service (TOS) and privacy policies for online apps and services used in the classroom;
- explaining to parents what, if any, personal information is shared with third parties and for what purpose(s); and
- publicly providing contact information for a staff person who can respond to questions about the school's data practices.

For more information on transparency, see PTAC's *Transparency Best Practices for Schools and Districts*, http://ptac.ed.gov/sites/default/files/LEA%20Transparency%20Best%20Practices%20final.pdf.

Colorado's Data Privacy Program

The Colorado Department of Education (CDE) has historically had strict standards regarding the care and utilization of individual student and staff data. In response to parental concerns, CDE organized a formal privacy program in 2015. The initial step to creating CDE's privacy program was to establish a team to address the intricacies surrounding data privacy. A key action was to employ a dedicated privacy staff person to focus on directing the work.

With the assistance of CDE's Data Management Committee, many new privacy resources were created and posted. The privacy team coordinated with the purchasing unit to revise contract language on a rolling basis to ensure that new privacy policy expectations were explicitly stated within each contract. Additionally, to increase transparency, any contract involving the sharing of personally identifiable information with a vendor is now required to include additional transparency language, specifically prohibit vendors from selling student data, and be posted on CDE's website.

To strengthen public trust and gather additional feedback, the agency's commissioner set up periodic privacy-focused public meetings. The CDE communications unit was intimately involved in revamping CDE's website to simplify, organize, and make privacy resources easier to navigate and access for constituents. Annual privacy training expectations were heightened as a 100 percent compliance rate was announced and achieved. Also, the Privacy Technical Assistance Center visited Colorado to provide professional development for local and state agency employees. A soon to be completed data privacy audit will provide a rich database of data elements collected along with related statutory authority.

CDE's next steps will include defining a departmental email/data retention policy, issuing a request for proposal for a security audit, and continuing to ensure the information security policies and practices are aligned with the department's evolving data privacy program. In addition, CDE will be working to analyze and implement the new state data privacy legislation.

Costs, Benefits, and Risks

Implementing privacy and security programs, training staff, and conducting audits all require time and money, both of which are in short supply at most education agencies. Unfortunately, unless they are required to do so by state or local board policy, some agency leaders may decide not to implement formal privacy or security policies and procedures until a data breach occurs or parents raise concerns. Ideally, agencies will consider the various components of privacy and security programs and implement the programs gradually as resources allow. Privacy and security programs will protect students from potential harm such as identity theft, discrimination, predatory activity, and emotional or social harm. They can also save the district from potential financial costs related to providing monitoring services for students in the event of identity theft, defending a lawsuit, and paying damages resulting from a lawsuit.

Staff Professional Development

Staff training is an important step in ensuring that student data are used and shared appropriately. In addition to security-related training, LEAs are responsible for training their schools' instructional and administrative staff—both employed and contracted—on data use, as well as procedures for properly acquiring and safely using online learning tools. Some LEAs require all staff, including teachers, to undergo training when they are first given access to student data. As staff are trained on how to use the student information system, they are also given basic training on privacy protections. Thereafter, annual training is helpful to reinforce important concepts and explain any changes to the systems. Many districts have official policies, sometimes called Acceptable Use Policies or Responsible Use Policies, which outline acceptable and prohibited activities for all categories of authorized data users (teachers, administrators, researchers, etc.). Staff may be required to sign a document stating that they understand the policy before gaining access to the data.

Most SEAs cannot bypass an LEA in offering training to school staff. However, depending on its resources, an SEA can offer training materials to its LEAs, or it can provide training sessions for school staff if the district requests assistance. Some SEAs offer a menu of training options from which LEAs and/or schools can select, depending on the time available for the training. (For example, see West Virginia's training menu at http://wvde.state.wv.us/forms/zoomwv/zoomwv_trainingmenu.pdf). PTAC offers a variety of training tools that can be customized for use by states and districts, which are available for free at http://ptac.ed.gov. In addition, depending on availability, PTAC staff might also be able to assist in conducting training sessions on FERPA requirements.

Privacy training programs for school staff may include the following topics related to the protection of student data:

- Definitions of "personally identifiable information" and "sensitive data"
- Federal legal requirements, including FERPA
- State legal requirements
- Local board policies related to privacy
- Directory information policies
- Appropriate uses and sharing of student data
- Authorized processes for managing data requests
- Protecting student privacy while using online educational services
- Methods for protecting PII in presentations and reports
- Data destruction best practices (e.g., shredding paper copies of student records, deleting files from computers or mobile devices)

Many districts consider in-person training to be preferable to online training because it allows for free discussion in a safe environment. However, if resources are limited, online training may be the best option. Both PTAC (http://ptac.ed.gov) and NCES (http://nces.ed.gov) offer materials that may be useful with staff professional development.

Roles and Responsibilities

Various entities and individuals are responsible for protecting the confidentiality of student information. Collaboration among state boards of education, local school boards, SEAs, LEAs, and schools is needed to design and implement effective privacy programs, policies, and procedures. Ultimately, everyone with access to student-level data has responsibility for ensuring that the data are used and shared according to agency guidelines. This section looks at some specific roles and responsibilities of entities and individuals.

State Boards of Education

The role of state boards of education in setting policies regarding student privacy varies across states. In general, however, state boards can recommend and adopt statewide education policies and provide guidance in adhering to privacy laws enacted by state legislatures. Most state boards of education are also responsible for overseeing the privacy practices of their state education agencies.

State Education Agencies

SEAs are responsible for protecting the data about P12 students that are stored in statewide data systems, and ensuring that all legal and ethical requirements are met when the data are shared with school districts, other state agencies, and research organizations. SEAs must also follow disclosure avoidance procedures when publishing aggregate student data in reports. In order to minimize access to sensitive information within the SLDS, the SEA is responsible for establishing data minimization best practices and implementing role-based access controls on all student-level information. For more information on disclosure avoidance, see http://ptac.ed.gov/sites/default/files/Case_Study_5_Minimizing_PII_Access.pdf.

SEA leaders are responsible for supporting data governance, data privacy, and data security efforts at the state level. In addition, SEAs can assist their LEAs—particularly small LEAs— by sharing information on how to establish data governance, data privacy, and data security programs and procedures. They can also provide resources and training opportunities for LEAs on how to comply with federal and state privacy policies.

Many SEAs negotiate agreements with vendors to provide statewide services. In these cases, SEAs are responsible for ensuring that vendors are in compliance with all privacy laws. SEAs should regularly monitor the terms of service and privacy policies for approved providers to ensure they have not changed. Some SEAs provide approved lists of vendors for use by LEAs within the state. Ultimately, however, LEAs are responsible for any contract with a vendor, and the LEAs must ensure that vendors are in compliance with all privacy laws, even if the SEA has pre-approved them.

Local School Boards

Local school boards may establish local policies for protecting student privacy that are no less restrictive than federal and state laws. They are also responsible for allocating the appropriate resources to enable schools to adequately protect the security and confidentiality of student data. School board members must understand the federal and state legal requirements for protecting student privacy, as well as the need to balance student privacy with the use of student data for innovative instructional practices.

Local Education Agencies

LEA staff are responsible for developing and adhering to privacy procedures that support federal, state, and local privacy requirements. LEA leaders are responsible for establishing and supporting effective data governance, data privacy, and data security programs that facilitate effective and innovative instructional practices. In addition, similar to SEAs, LEAs are responsible for instituting role-based access controls to protect data. LEAs must regularly review their policies and practices to be sure they are consistent with any changes in legal requirements or any changes in the technologies being used. LEAs are also responsible for ensuring that agreements with district service providers are in compliance with privacy, security, and appropriate data-use requirements.

It is important for LEAs to provide professional development for all LEA and school staff on the topics of data privacy and security. All LEA staff who have access to student data are responsible for following LEA guidelines for protecting student data.

Another responsibility of LEAs is appropriately responding to data requests from outside the agency, and ensuring that any distribution of information complies with all applicable privacy laws and policies. It is a best practice for districts to have standardized processes for receiving, reviewing, and processing requests.

School Staff

School staff are responsible for following procedures set by their LEAs and providing feedback on the practicality of the procedures. Principals play an important role in communicating the importance of protecting student privacy. Principals can ensure that school staff have access to appropriate training. They can also support the use of consequences for staff failure to follow privacy and security protocols. If denying access is not practical as a consequence, then principals may want to consider the use of oral or written reprimands to enforce adherence to privacy and security protocols. School staff, particularly teachers, are responsible for teaching students the importance of protecting their personal information when using online tools and programs. In light of the ready availability of freeware that can be used in the classroom, teachers are ultimately responsible for understanding how the online applications they use in the classroom may be collecting data about their students, and whether or not these collections are appropriate. If they are not certain, the teachers are responsible for requesting assistance in evaluating the application. Teachers are also responsible for modeling and teaching good digital citizenship to their students throughout the year.

Checklist for Staff with Access to Student Data

- ✓ Ask for and attend training on data privacy and security.
- ✓ Identify barriers to effective data protections and communicate these to appropriate personnel.
- ✓ Respect the privacy and confidentiality of student data by protecting data from unauthorized use.
- ✓ Follow your district data security policies and procedures (e.g., change passwords at regular intervals, do not share passwords with colleagues or students).
- ✓ Ask for help if you believe student data have been inadvertently made available to unauthorized individuals.
- ✓ Share best practices for protecting student data with your peers.

Parents and Students

Parents can help ensure that schools and districts are appropriately protecting student privacy. Parents can seek out information on how a school uses student data and protects the confidentiality of those data. If this information is not readily accessible on a school website or through other school communication channels, parents can ask their schools and districts for the information. Parents can also model and teach their children responsible digital citizenship.

Students are responsible for protecting their logon credentials (e.g., user name and password) for all school-sponsored systems, including e-mail and online learning management systems. Students are also responsible for not disclosing personal information about themselves or other students to unauthorized individuals.

Vendors/Third-Party Service Providers

Organizations and companies that provide services to education agencies need to be aware of their responsibilities to protect student data. A memorandum of understanding or other clear agreement is needed to explicitly describe how the service provider will appropriately access, use, share, and destroy student data. All third-party staff who work with student data need to be trained on their responsibilities; some education agencies may also require these individuals to sign individual confidentiality and non-disclosure agreements. Service providers need to prominently post their privacy practices in plain language on their websites and provide a reliable point of contact on their website for questions pertaining to privacy and security. Links to their privacy policies and points of contact need to be maintained in good working condition so they can be easily accessed.

Teacher Preparation and Certification Programs

Given the widespread use of student data in the classroom today, teacher preparation programs ideally will train teacher candidates in the appropriate use of student data, including the legal requirements for protecting those data. Teacher certification programs can do their part to ensure that new entrants to the field of teaching demonstrate knowledge of the legal requirements and appropriate use of student data before granting certification.

Chapter 2:
Case Studies in Protecting Student Privacy

This chapter presents 11 case studies highlighting common practices in schools that may jeopardize student privacy. Each of the 11 case studies includes the following sections:

- A scenario (or vignette) that depicts common situations in many districts and exemplifies the critical issue discussed in the case study
- A statement of the "best practice challenge" presented in the scenario
- Examples of how some districts are managing the challenge
- Lessons learned in managing the challenge
- Action steps education agencies may want to consider
- Related case studies

The case studies are designed to be used independently as catalysts for thoughtful discussions on a single issue. However, many of the case studies are interrelated and cross-references are included to help the reader determine which case studies are best used together. The case studies may be helpful in raising awareness and sparking dialogue on privacy concerns primarily at the school and LEA levels. SEAs may also find many of the case studies relevant to privacy issues within their agencies. In addition, SEAs may want to use the case studies when working with LEAs on developing privacy programs or training sessions.

It is important to note that privacy practices are complicated, and no single case study or even group of related case studies will necessarily present a comprehensive solution to managing the confidentiality of student data. In addition, state privacy laws and local board policies vary, so successful methods for addressing the privacy concerns presented in the case studies will also vary. The information presented in the case studies is not intended as legal guidance. In all cases, appropriate internal experts—such as privacy coordinators, information technology (IT) staff, legal staff, and purchasing staff—should be consulted to determine specific best practices for a particular agency.

A recurring theme in the case studies is the need for staff professional development. All staff members who are given access to student data need to be properly trained on appropriate data use and security measures. In addition, classroom teachers need training on how to safely choose, acquire, and use online learning tools in keeping with district policy. Improper use of data by school staff is typically due to lack of training or unintentional errors or oversights. Staff who are found to misuse data or inappropriately share student data may need repeated training opportunities, supervisor counseling, and/or written reprimands to emphasize the importance of the appropriate use and safeguarding of student data.

Case Study #1: Using Online Learning Applications in the Classroom: Decentralized Review

Perhaps nowhere else is the tension between privacy requirements and instructional needs stronger than in the use of online learning applications (apps) in the classroom. Often, vendors may bypass the district office and direct their sales pitches to teachers. Some online apps are available for free or very low cost, which makes it easy for teachers to acquire and use the apps. However, under FERPA, school districts are responsible for maintaining direct control over all vendors with respect to the use and maintenance of education records. Therefore, some districts now require a formal review and approval by authorized staff before a teacher can use any new online app with students. Other districts, however, do not have the resources to provide this kind of central review. This case study examines how districts that do not provide a central review process for new online apps can support teachers in responsibly selecting and using new online apps in the classroom.

Scenario

Ms. Smith is a fifth-grade teacher in the Washington County Public Schools district. A vendor has contacted her about a free online app she can use to help teach her social studies class about the American presidents. The only thing she needs to do is locate the app online and set up accounts for her students with their names and e-mail addresses. The students will then each have a personalized instructional account through which they can access the online material. The online program presents instructional content aligned to specific state social studies standards, along with quizzes to assess student learning. The teacher can download a report from the program that summarizes each student's progress.

Ms. Smith accesses the online software, enters the students' names and e-mail addresses to set up their accounts, and introduces her students to the new instructional tool the following day. The students enjoy the new app and improve their understanding of the American presidency. So Ms. Smith is concerned when Ms. Jones, the school principal, announces during a staff meeting that the district has instituted new procedures teachers must follow before using any new online app in the classroom. She tells Ms. Jones that she suspects the new procedures will unnecessarily impede her efforts to offer timely, effective, engaging and personalized instruction to her students. Ms. Jones is sympathetic because she knows her teachers are very busy. She also knows, however, that the district is responsible for ensuring that student data collected through online learning apps are properly used and protected.

Best Practice Challenge

Some districts have insufficient staff resources to assist teachers in reviewing new instructional apps for privacy considerations. How can these districts facilitate the use of these apps by teachers while also protecting student privacy?

District Practices

- Some districts offer guidance to teachers on how to review new instructional apps. The first step in determining whether an online app should be used in the classroom is evaluating its instructional value. Districts may provide a list of questions teachers can ask to determine if a new app is likely to be helpful in a classroom. The questions might include the following:

  a. Is the app instructionally meaningful to my students?
  b. Does it encourage 'creating' and 'problem-solving' rather than passive use?

  If the answers are yes, then the app should be reviewed for privacy considerations.
- In many cases, the new online apps that teachers are seeking to use are commonly known as "clickwrap apps." These are free or low-cost apps that require the user to click "I agree" to the vendor's online terms of service (TOS) and privacy policy before the app can be used. These agreements are generally considered to be legally

enforceable. Listed in the box below are suggested guidelines for reviewing the TOS and privacy policies for online learning applications, including clickwrap apps.

- Many districts require teachers to obtain parental consent before using any new online app in the classroom. By obtaining parental consent, a FERPA violation is much less likely to occur.
- Districts may provide a standard release form for teachers to use at the beginning of the school year in obtaining parental approval for their students to use online instructional apps. The teacher can use the form to describe the types of learning apps that are planned for use during the year, and include a link to the TOS for each app. If the school district has the technical capabilities, the district can mechanize the approval process so that parents can electronically approve the request and staff can check the system to see which parents have provided approval. A mechanized process will greatly reduce the time and effort needed to obtain and check parental approvals. If a teacher decides to use additional online instructional apps not covered under the initial release, the teacher will need to contact parents to obtain approval for their students to use each new app. Ideally, the teacher will include a link to the TOS for the new app when requesting parental approval.
- Many districts advise teachers to download a copy of the TOS and privacy statement for each online app they are using with students. They also ask teachers to provide a list of all online apps they are using with students to a designated contact person within the school or district. This helps the district keep track of all online instructional apps being used with students in the district.

Guidelines for Reviewing Online Instructional Apps for Privacy Considerations

- Student information and academic content should be contained within a password-protected environment or controlled by teacher invitation, and not discoverable by search engines or publicly viewable on the internet.
- If the app requires the use of student PII such as name, e-mail address, or student identifier, parental approval may be required.
- Check the Terms of Service (TOS) and Privacy Policy for the following:
    a. Are there age restrictions on the use of the software? If the software is not intended for use by children under 13 years of age, it cannot be used in classes where there are children under 13. If the app is appropriate for use with children 13 or older, parental consent may still be needed. (For more information, see the FTC's Complying with COPPA: Frequently Asked Questions at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.)
    b. Are all student data securely maintained, used only for educational purposes, and not shared with any other organizations?
    c. Do the modification provisions allow the provider to make a material change in the TOS or Privacy Policy without providing notice or requiring consent from the school/district? Avoid using apps with this kind of provision.
    d. Is it clear that the data collected cannot be used to advertise or market to students?
    e. Often the TOS will begin with defining PII or student data that will be used throughout the agreement. A broadly written definition of personally identifiable information can help ensure that more information is included and protected. For example, a TOS that defines PII as "only user information knowingly provided by the user" is too narrow. The vendor is only obligated to protect that specific information. A better definition would be "information provided by or about students, metadata, and user content."
    f. Be wary when the TOS talks about using de-identified data for other purposes. It can be difficult to completely de-identify data.
    g. Beware of any statement indicating that providers may view access to their services through a third-party site as an exception to established rules limiting data collection.
    h. A pro-privacy TOS will specify the types of data (or specific data elements) that the service may collect.
    i. Make sure the TOS agrees with all applicable federal, state, local or tribal laws.

For more information, see Protecting Student Privacy While Using Online Educational Services: Model Terms of Service.

Lessons Learned

- Security policies and procedures should support instruction, not impede it.
- When working with instructional staff, emphasize the positive aspects of what security precautions can do for them and their students.
- Anticipating instructional needs with readily available pre-approved products or clear procurement procedures can minimize the degree to which privacy impedes instruction.
- Some staff may question why they need permission to use online learning apps when they only need to provide student names and e-mail addresses. These data elements are typically considered directory information. Thus, some staff may believe no parental consent should be needed. It should be made clear to staff that once data elements considered to be directory information are combined with any other information about students as part of a school activity, the directory exception under FERPA may no longer apply. Online learning apps routinely collect student learning data and are combined with the student's name.

Action Steps

- ✓ Review your agency's policies and procedures on the use of online instructional tools.
- ✓ Review the information on COPPA found in Chapter One in the section on Federal Privacy Laws.
- ✓ Download the following free resources available at http://ptac.ed.gov:
  - ▪ Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf
  - ▪ Protecting Student Privacy While Using Online Educational Services: Model Terms of Service http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf

Related Case Studies

Case Study #2 discusses how new online apps may be reviewed in districts with a centralized review and approval process. It includes best practices for contracting with third-party providers of online instructional apps.

Case Study #2: Using Online Learning Applications in the Classroom: Centralized Review

Under FERPA, school districts are responsible for maintaining direct control over vendors with respect to the use and maintenance of student PII from education records. This control must be demonstrated when districts want to share student data with vendors. Some states have recently passed laws that shift at least some of the responsibility for protecting student data to the vendor. However, it is important for districts to have strong agreements in place with vendors that specifically outline the approved uses of the data as well as the responsibilities for protecting student privacy.

Contracts (also "service agreements" or "memoranda of understanding") are used with service-providers to specify

- the services that will be provided;
- the data to which the service provider will have access;
- approved uses of the data, possibly including specific examples of how the data cannot be used;
- requirements to protect the confidentiality of the data and the privacy of the students; and
- guidelines for how the data should be destroyed once they are no longer needed.

A good contract will include all of the information listed above. The contract may include some of this information under the specific headings of "terms of service," "end-user license agreement," and/or "privacy policy."

Given the growth in online instructional tools that teaching staff are eager to acquire—sometimes for free—significant staff time could be needed to prepare and/or review service-provider contracts. Districts need to find efficient ways to manage contracts as well as train instructional staff on district policies for entering agreements with online vendors. This case study looks at how districts can effectively manage vendors of online instructional apps and efficiently review new apps requested by instructional staff.

Scenario

Ms. Jones, the new privacy coordinator in the Jackson County Public School District, is feeling a little overwhelmed. Legally, the district is responsible for how student data are used when they are shared with a third party. Due to growing parental concerns about the expanding use of online instructional applications (apps) in the classroom and vendor access to student information used in the apps, the district has established new rules governing the use of those apps. Even freeware (online apps that teachers can download and use for free or a nominal charge) must now be reviewed by the district's privacy committee. The number of requests from teachers to use new online apps has been growing. Ms. Jones is pleased that school principals have gotten the word out about the new policy and that teachers are following the rules, but the privacy committee simply does not have the time to review all of the requests they are receiving. The privacy committee is comprised of staff from the information technology (IT), data management, legal, and purchasing departments. Under the committee's current procedures, freeware is reviewed by a committee member to determine the types of student information that will be used in the app, and the vendor's online terms of service (TOS) and privacy policy to which a teacher must agree (by clicking "I Agree") before the app can be used. These are known as "clickwrap" agreements and are generally considered to be legally enforceable. Committee members are trained in reviewing the software for important considerations, including looking for language in the TOS that clearly states the data collected cannot be used to advertise or market to students and other important considerations. The backlog of approval requests is growing, and Ms. Jones decides the committee must come up with a better way to manage the review process.

Best Practice Challenge

How can districts efficiently ensure that all online service providers that use or collect student data will only use the data for approved purposes and protect the confidentiality of the data?

District Practices

- Many districts maintain a list of pre-approved online apps for use in the classroom. As new apps are formally approved, they are added to the list.
- Some districts have developed boilerplate agreements for online apps, standard language for TOS, and/or standard contracts for standard services from vendors. All staff who are authorized to negotiate contracts on behalf of the school district need to be aware of these standard forms and use them consistently.
- Some districts have adopted a contracting process for online apps similar to the one outlined below:
    a. Teachers notify a designated staff member when they identify an app that they would like to use that is not included in the list of pre-approved apps.
    b. The designated IT staff member sends the district's standard contract for online services to the vendor and notifies the vendor that a teacher would like to use the app but cannot do so until the standard contract is in place.
    c. Once the vendor signs the contract and returns it to the district, the teacher can begin using the new app. If the vendor does not want to sign the district's standard contract, and the online app is related to a core piece of the curriculum and useful to a number of teachers, the legal department may become involved in negotiations with the vendor to reach an agreement.
- Some districts have developed databases that provide an analysis of vendors' standard TOS to aid in the review process.
- Some districts require an official review by other instructional staff (in addition to the requesting teacher) to confirm the instructional value of the software before privacy concerns and vendor agreements are reviewed.
- Some districts will agree to use a vendor's standard contract as long as the vendor has signed an industry pledge, such as the Software & Information Industry Association/Future of Privacy Forum (SIIA/FPF) Student Privacy Pledge. More than 200 companies have signed the pledge, which is legally enforceable under the Federal Trade Commission (FTC) and consumer protection laws. Note that enforcement only applies to the for-profit companies who have signed the pledge; the FTC is generally not involved in monitoring nonprofit activity. Since LEAs are ultimately responsible for ensuring that all contracts protect the privacy of student information, LEAs may choose to consider a vendor pledge as a first level of review but still review the vendor contract before signing it.
- Some districts are working as part of consortia to manage privacy and security issues related to online services and products. For example, the Massachusetts Student Privacy Alliance (MSPA) is a statewide collaboration of school districts that share common concerns around student privacy (https://secure2.cpsd.us/mspa/index.php). One outcome of that collaboration has been the adoption and implementation of a common Student Data Breach Contract that can be used by all member schools when implementing any online app.[4] At the national level, the Access 4 Learning Community (formerly the SIF Association) launched a student data privacy consortium in late 2015. The consortium is focused on "operationalizing the complex and high-profile privacy and security issues surrounding the safeguarding of student data" by sharing and replicating best practices among participating education agencies and software vendors (A4L 2015).

[4] See https://secure2.cpsd.us/mspa/about_mspa.php

Guidelines for Reviewing Online Instructional Apps for Privacy Considerations

- Student information and academic content should be contained within a password-protected environment or controlled by teacher invitation, and not discoverable by search engines or publicly viewable on the internet.
- If the app requires the use of student PII such as name, e-mail address, or student identifier, parental approval may be required.
- Check the Terms of Service (TOS) and Privacy Policy for the following:
  a. Are there age restrictions on the use of the software? If the software is not intended for use by children under 13 years of age, it cannot be used in classes where there are children under 13. If the app is appropriate for use with children 13 or older, parental consent may still be needed. (For more information, see the FTC's Complying with COPPA: Frequently Asked Questions https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions)
  b. Are all student data securely maintained, used only for educational purposes, and not shared with any other organizations?
  c. Do the modification provisions allow the provider to make a material change in the TOS or Privacy Policy without providing notice or requiring consent from the school/district? Avoid using apps with this kind of provision.
  d. Is it clear that the data collected cannot be used to advertise or market to students?
  e. Often the TOS will begin with defining PII or student data that will be used throughout the agreement. A broadly written definition of personally identifiable information can help ensure that more information is included and protected. For example, a TOS that defines PII as "only user information knowingly provided by the user" is too narrow. The vendor is only obligated to protect that specific information. A better definition would be "information provided by or about students, metadata, and user content."
  f. Be wary when the TOS talks about using de-identified data for other purposes. It can be difficult to completely de-identify data.
  g. Beware of any statement indicating that providers may view access to their services through a third-party site as an exception to established rules limiting data collection.
  h. A pro-privacy TOS will specify the types of data (or specific data elements) that the service may collect.
  i. Make sure the TOS agrees with all applicable federal, state, local or tribal laws.

For more information, see Protecting Student Privacy While Using Online Educational Services: Model Terms of Service.

The SIIA/FPF Student Privacy Pledge. In 2014, the Software & Information Industry Association (SIIA) and the Future of Privacy Forum (FPF) introduced a voluntary vendor pledge to safeguard student privacy. The pledge applies to all student personal information whether or not it is part of an “educational record” as defined by federal law, and whether it is collected and controlled by the school but warehoused offsite by a service provider, or collected directly through student use of a mobile app or website assigned by their teacher. It also applies whether or not there is a formal contract in place between the school service provider and the school. Companies that violate their pledge may be subject to action by the Federal Trade Commission as deceptive trade practices. By signing the pledge, school service providers promise they will

- not collect, maintain, use, or share student personal information beyond that needed for authorized educational/school purposes, or as authorized by the parent/student;
- not sell student personal information;
- not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students;
- not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student;
- not make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data are used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements;
- not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student;
- collect, use, share, and retain student personal information only for purposes authorized by the educational institution/agency, teacher or the parent/student;
- disclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student personal information they collect, if any, and the purposes for which the information is used or shared with third parties;
- support access to and correction of student personally identifiable information by the student or their authorized parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent;
- maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks—such as unauthorized access or use, or unintended or inappropriate disclosure—through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information;
- require that other vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments for the given student personal information; and
- allow a successor entity to maintain the student personal information, in the case of a merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student personal information.

For more information, see https://studentprivacypledge.org/.

Lessons Learned

- Instructional staff need to be given a general timeframe in which they can expect to receive a response to a software app approval. They also need to understand what the process entails and why it is necessary.
- Vendors may sometimes initially agree to use a district's standard contract, but then include an addendum with the signed contract that essentially overrides the TOS outlined in the district's contract. Districts need to carefully review any addendum that a vendor attaches to its standard contract.
- Many reputable vendors with quality education products may be hesitant to use a district's standard contract because they are required to use the contract language prepared by their legal departments. If the app is deemed by the district's instructional experts to be of high quality and potentially useful to many teachers in the district, then it may well be worth the time and effort to work with the vendor to develop a contract that can be approved by the legal counsel of both parties.
- Not every district has a legal department, but those districts that have one may find that the legal department must be involved in the development of all contracts, service agreements, or memoranda of understanding.
- Many districts have found that sharing information through cross district consortia or national consortia can help reduce the burden of reviewing and monitoring vendor agreements.

Action Steps

- ✓ Ask if your SEA or LEA recognizes the SIIA/FPF Vendor Pledge.
- ✓ Download PTAC's Protecting Student Privacy While Using Online Educational Services: Model Terms of Service from http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services-model-terms-service.

Related Case Studies

Not all districts have the resources to support a centralized review process for new online apps. Case Study #1 discusses general practices a district can adopt to assist teachers in reviewing online apps for use in the classroom when a centralized review process is not available.

Case Study #3: Parent Requests for Student Contact Information

This case study looks at a common request for directory information that many teachers receive: the parent of one of the students within a classroom is requesting contact information for other students in the class. How a teacher responds to this type of request will depend on the district's directory information policy.

Scenario

Lily Bennett is a first-grade student at Adams Elementary School. Her mother is hosting a birthday party for Lily and wants to invite all of the students in Lily's class. Lily's mother sends an e-mail to Lily's teacher, Mrs. Jordan, requesting the names and addresses of all students in Lily's class. Mrs. Jordan is a first-year teacher. She wants to encourage friendships among the students in the class, and she likes the fact that Lily's mother plans to include all of the children. Mrs. Jordan remembers hearing something about restrictions on sharing student contact information in the training she received when she was given access to the district's student information system, but she thinks names and addresses are okay to share with anyone who requests them. To be safe, she decided to check with the school secretary.

Best Practice Challenge

How can a school ensure that teachers follow district privacy guidelines when responding to requests for student contact information from parents or volunteers who are hosting parties to which students are invited, preparing personalized treats for class members or student name badges for field trips, or promoting class events?

District Practices

- Some districts train teachers on the district's directory information policy and the appropriate sharing of student contact information at the time the teachers are learning how to use the data system and are given their log-in information. Teachers may be required to sign an affidavit at the end of each training saying they understand the restrictions on the use and sharing of student data. If the request falls within the district's directory information policy, the teacher must check to see if any parents have opted out of sharing their children's information before responding to the information request. Teachers are advised that if they receive a request from a parent that falls outside of the district's directory information policy, then they must send a request to the parents of all students in the class either asking for written permission to share their children's contact information with the other parent or encouraging parents to directly contact the parent requesting the student contact information.

FERPA Directory Information Exception

Under FERPA's directory information exception, schools may disclose student information that is classified as directory information without the consent of the parent or eligible student. However, schools must tell parents which data are considered directory information, and allow parents a reasonable amount of time to opt out of sharing their child's information. Schools generally provide parents with examples of how the information may be used, such as honor roll lists, yearbooks, and athletics programs. Agencies have the option to adopt *a limited directory information policy*, under which schools must tell parents the specific purposes for which the data will be used or specific organizations with whom the data will be shared. Under both directory policies, schools are not required to allow parents to pick and choose the types of directory information that can be shared, or the specific uses for which they do not want their child's information shared. However, some districts have chosen to provide this kind of flexibility and allow parents to opt in or out of specific uses for directory information.

It is important to note that as soon as data elements designated as directory information are combined with non-directory information, the directory exception under FERPA will no longer apply.

- Some schools include in the back-to-school paperwork permission forms for each of the student's teachers requesting the parents' permission to include student names and parents' contact information in a class directory to be shared with members of the class.
- To reduce the time required for teachers to check for parents who have opted out of sharing directory information, some districts include this information in the student information system. Teachers can conduct a search for specific students to determine the status of the directory information opt-outs. In addition, some districts offer a standard, mechanized process for collecting parental consents for specific data uses during the school year. Parents can electronically respond to the request for data sharing, and staff can check the system to see which parents have provided or withheld consent.
- Some districts put the directory information and opt-out policies in the district student handbook that every student receives on the first day of school and all new students receive when they enroll. This helps ensure that every family receives the information.

Lessons Learned

- Parents are more likely to agree to sharing e-mail addresses than home addresses or phone numbers when contact information is requested by other parents.
- Parent, not student, e-mail addresses should be shared with other parents when contact information is needed.
- It is helpful for districts to note in a student information system any orders of protection or other court orders for children that may be in place at the beginning of the school year, or are received later in the year. These orders may have implications for information-sharing.

Action Steps

- ✓ Review the district's directory information policy to determine if it covers parent requests for student contact information.
- ✓ Based on the district's directory information policy, prepare specific guidance for teachers on how to respond to parent requests for student contact information.

Related Case Studies

Case studies #4 and #11 also pertain to the sharing of directory information. Also, see the section on Federal Laws in Chapter One for an overview of directory information policies under FERPA.

Case Study #4: PTA Requests for Student Contact Information

This case study looks at a common request for directory information that schools receive: the Parent-Teacher Association asks for contact information for the parents of all students in the school in order to promote a schoolwide event. How a school responds to this type of request will depend on the district's directory information policy.

Scenario

The Parent-Teacher Association (PTA) at Quincy Middle School is introducing a special science incentive program for students. Ms. Lowe, the PTA program coordinator, is a neighbor and good friend of the new school secretary, Ms. Norton. She asks Ms. Norton for the names and addresses of all parents of enrolled students in order to send them information about the program. Ms. Norton is aware that the PTA fundraiser information was included in the back-to-school packets that all parents received. She is not certain how to handle other PTA communications, however. She knows most of the parents at the school would be interested in the new program, but she also knows from her training on how to use the data system that there are certain limitations on who can receive directory information. She wants to help her friend, but isn't sure if the rules allow her to. Although it is difficult for her to do so, she tells Ms. Lowe that she needs to check with the principal before releasing the information.

Best Practice Challenge

How can a school facilitate timely communications with the parents of all students in order to support parent groups or community-supported schoolwide events or activities without violating privacy requirements?

FERPA Directory Information Exception

Under FERPA's directory information exception, schools may disclose student information that is classified as directory information without the consent of the parent or eligible student. However, schools must tell parents which data are considered directory information, and allow parents a reasonable amount of time to opt out of sharing their child's information. Schools generally provide parents with examples of how the information may be used, such as honor roll lists, yearbooks, and athletics programs. Agencies have the option to adopt *a limited directory information policy*, under which schools must tell parents the specific purposes for which the data will be used or specific organizations with whom the data will be shared. Under both directory policies, schools are not required to allow parents to pick and choose the types of directory information that can be shared, or the specific uses for which they do not want their child's information shared. However, some districts have chosen to provide this kind of flexibility and allow parents to opt in or out of specific uses for directory information.

It is important to note that as soon as data elements designated as directory information are combined with non-directory information, the directory exception under FERPA will no longer apply.

District Practices

- Some districts include on the student enrollment form a box that parents can check to grant approval to share parent contact information with the PTA. Since all parents must complete and sign the student enrollment form, the district is more likely to get responses from parents on the data-sharing request than if the district used a separate form to make the request. In addition, some districts include in the student information system an indicator as to whether or not the parent has provided approval.
- Some schools post PTA-related forms on the school website.
- At the elementary level, schools may ask the PTA to prepare informational fliers to be distributed to all teachers and sent home in student backpacks. This approach does not work as well at the middle or high

school levels. At these levels, if the PTA has sufficient funds to pay for postage, the school secretary can ask the PTA to organize the mailing (i.e., prepare the information to be mailed and apply postage to the mailers), and the school secretary can apply address labels and mail the information packets.

Lessons Learned

- The school secretary generally has greater access to student information than almost any other school staff member. Therefore, school secretaries need extensive training on the district's directory information policy and related issues of appropriate data use.
- In many schools, the PTA coordinator develops close relationships with school staff. This may make it difficult for school staff to enforce rules on data sharing. Ideally, the school will work with the PTA to inform PTA volunteers about restrictions on sharing parent and student contact information.

Action Steps

- ✓ Review the agency's policy on directory information regarding sharing contact information with the PTA.
- ✓ Be sure that school secretaries are trained on how to respond to PTA requests.

Related Case Studies

Case studies #3 and #11 also pertain to the sharing of directory information. Also, see the section on Federal Laws in Chapter One for an overview of directory information policies under FERPA.

Case Study #5: Staff Presentations That Include Student Data

With a few exceptions, FERPA prohibits schools from disclosing personally identifiable information (PII) from student education records to a third party without written consent from the parent or eligible student. PII includes information that can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information. Direct identifiers include information that relates specifically to an individual such as the individual’ s name, address, Social Security number, telephone number, e-mail address, or biometric record. Indirect identifiers include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, place of birth, race/ethnicity, religion, weight, and/or school activities. Thus, when education staff are sharing information about the impact of education programs on student progress, or demonstrating new data tools to monitor student achievement, steps should be taken to protect the student data used in the presentations so that no individual student can be identified. This case study looks at how education agency staff can use actual student data in presentations without risking the disclosure of student identifiable information.

Scenario

Dr. Shawn Wilson is responsible for developing the early warning system for his district. He has been invited to discuss the new system at an annual conference of data professionals. He uses actual student data in his presentation, but he knows he needs to ensure that no individual student can be identified from the information he presents. So, he deletes the last name of all students. Meanwhile, one of his peers, Dr. Judy Snow, is also presenting at the same conference on her district’s new intervention program for at-risk students. Dr. Snow happens to pull the same student data to use in her presentation. Like Dr. Wilson, she knows she needs to protect the confidentiality of the data she uses in her presentation, so she only uses the last names of students in her presentation. Thus, the potential exists for conference-goers to piece together the full names of students from the two presentations.

Best Practice Challenge

How can education staff protect student privacy when using actual student data in conference presentations or staff trainings?

District Practices

- In some districts, staff members are instructed to de-identify the student data they use for trainings or presentations by substituting fictitious names for real student names, and/or fictitious student identifiers for real student identifiers. Using fictitious data is the best way to prevent unintended disclosures.
- In other districts, staff members are instructed to remove all direct identifiers (names, identification numbers) from the data by masking the names or numbers.
- In addition to preventing the disclosure of direct identifiers such as names and student identification numbers, staff must also prevent the disclosure of individual student data through indirect identifiers. The goal is for a reasonable person not to be able to identify an individual student based on the data shown. Thus, staff are also instructed to use a consistent minimum size for a data group when reporting aggregate data so that individual identities cannot be deduced from a small number of students.

Lessons Learned

- Using part of a name only (e.g., first or last name but not full name) is problematic even when there is no chance the two names may be revealed in separate presentations. Some names are unique and anyone with general knowledge of a school may be able to recognize a student by part of their name only.
- Standard procedures help prevent accidental identification of student information. Stay consistent within your LEA/SEA when releasing training or public data so as to prevent disclosure.
- Vendor demos are another situation in which student privacy may be jeopardized. Some vendors may demo software by showing the work they have done for another district unless they are specifically asked not to do so.

Action Steps

- ✓ Check to see if your district has a standard policy on how to protect student PII in training materials or public reports.
- ✓ Download and read the Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records, available from the National Center of Education Statistics at http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601.
- ✓ Download and read the Frequently Asked Questions: Disclosure Avoidance and Data De-identification: An Overview of Basic Terms available from the U.S. Department of Education's Privacy Technical Assistance Center at http://ptac.ed.gov/sites/default/files/FAQ_Disclosure_Avoidance.pdf and http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf.

Related Case Studies

Case studies #6, #7, #8, and #9 also pertain to appropriate sharing of data within a school.

Case Study #6: Posting Personally Identifiable Student Data Within the Classroom or School Building

It is common practice for teachers to post outstanding student work in schools and classrooms to showcase student talent. This type of display of student work is considered by some districts to be covered under FERPA's directory information exception for sharing honor roll information. In some cases, however, instructional staff may be posting student performance data as a way to monitor student progress. This case study looks at the practice of posting personally identifiable student performance data within a school for the purpose of allowing teachers to discuss performance.

Scenario

The teaching staff at Jefferson Middle School are proud of how they use student data to inform instructional practices. Teachers have created "data walls" by posting charts showing student performance data in classrooms and multi-use areas of the school where staff meetings are held. This allows teachers to easily see how students are progressing. Some of the data charts include only aggregate data on overall classroom progress. But other data charts—primarily those used for team teaching purposes—include sensitive, student-level data such as attendance, discipline, and assessment scores. When the principal, Mr. Ross, raised concerns about displaying this type of information, the teachers decided to cover the walls when they were not being used. Mr. Ross still has some concerns about this, because some of the data walls are in an unlocked, multi-use area of the school. He considers asking the teachers to move the data charts to meeting rooms that can be locked, but he knows that cleaning staff can still gain access to those rooms. He decides to talk to his colleagues about other options for how teachers can appropriately share data for this purpose.

Best Practice Challenge

How can teachers appropriately share sensitive, student-level data with each other to plan instruction and intervention services?

District Practices

- Some districts and states provide web-based tools that allow teachers to create electronic data charts filtered on specific students. Teachers can use a projector to display the files as needed, and once the meetings are over, the data are no longer visible. Electronic files should be encrypted or password-protected, and the filter should be set so that teachers are restricted to seeing only the students for whom they have responsibility.
- Some districts encourage the use of non-identifying student numbers rather than student names in the charts. If student names are needed for the analysis, one teacher could have (and protect) the data key that relates the random numbers to student names. Caution needs to be used to ensure that students cannot be identified based on the data in the display. For example, the only Hispanic student in the class could be identified if racial and ethnic data are shown.
- Whether the chart is shared on paper or electronically, once it is no longer needed the chart and all of the data contained in it should be destroyed. Paper copies should be shredded or incinerated. Electronic documents should be permanently deleted.

Lessons Learned

- Teachers are willing to use data, but the data must be made available in ways that are quick and easy to use.
- Some teachers prefer working with paper charts and manually updating information so that they do not need to get a projector to display the information each time they meet. These teachers need to understand the risks

involved in using paper charts. Charts that display student-level, personally identifiable, sensitive information should not be posted where unauthorized persons may have access. In addition, once the charts are no longer needed, they should be shredded so that they do not fall into the hands of unauthorized users.

Action Steps

- ✓ Train teachers on the appropriate ways to display student data (or student work) in the classroom or school building.
- ✓ Make projectors and other A/V equipment readily available to teachers, along with easy-to-follow instructions on how to use the equipment.
- ✓ Teachers who prefer to use paper displays should be trained on the importance of sharing student data only with other authorized users. Paper charts used in meetings should be removed from display after the meeting and stored in a locked cabinet. Once the chart is no longer needed, it should be shredded to prevent unauthorized access to the data.

Related Case Studies

Case studies #5, #7, #8, and #9 also pertain to appropriate sharing of data among instructional staff. For more information on data destruction, see the section on staff security training in Chapter 1.

Case Study #7: Teacher-to-Teacher Sharing of Student Data

FERPA allows student data to be shared with anyone considered to be a school official who needs to access a student's data for educational purposes. Districts vary in how they define school official, as well as the amount of student data to which individual school officials have access. All teachers, however, will need to access student data during the school year, even if they are only given access to the students in their classrooms. Teachers must take care to use the data only for instructional purposes. This case study looks at appropriate ways in which teachers can access and share student data.

FERPA School Official Exception

FERPA allows student data to be shared with anyone considered a school official who needs to access a student's data for educational purposes. Districts vary in how they define "school official," as well as the amount of student data to which individual school officials have access. The district's annual notification to parents and eligible students regarding their rights under FERPA should be used to explain how the district defines school official.

Scenario

Ms. Hutchins is a new math teacher at Lincoln High School. She needs advice on how to help a student who is struggling in one of her classes. She brings the student's most recent graded test to a meeting of the math department in order to seek advice from other teachers. She circulates the student's test among the other teachers so they can help analyze where the student is failing to grasp the underlying concepts. One of the more experienced teachers in the group reminds Ms. Hutchins that within their school, only teachers who work directly with a student are able to view that student's data. She suggests that Ms. Hutchins cover the name of the student before circulating the test.

Best Practice Challenge

How can a district support teachers in accessing and sharing data appropriately for instructional purposes without violating the minimum necessary standard under FERPA of who needs access to the data?

District Practices

- Some districts establish a consistent policy for use by all schools that outlines who falls under the definition of school official along with approved data use guidelines for those officials.
- Other districts allow each building administrator to decide who is responsible for the education in their building and therefore should be considered school officials. Some districts may decide that all teachers and aides are responsible for all students as a community. Others decide it is by grade level, or just the students assigned to a specific teacher. This decision needs to be clearly communicated and enforced within each building.
- The annual FERPA notification to parents is used to identify school officials who will be given access to student data as needed, such as teachers, counselors, student teachers, substitute teachers, peer tutors, volunteer tutors, and so on.
- Teachers are trained annually on (a) the prohibition against using student data for non-educational purposes, and (b) how to share student information for collaborative teaching purposes without disclosing the identity of the student. Potential consequences for violating the policy include
  - additional training requirements,
  - counseling sessions, and/or
  - written reprimands.
- Staff training on data use and student privacy can be presented during orientation or offered electronically through the district's learning management system.

Lessons Learned

- Staff rarely misuse student data for malicious purposes, but it is important to hold staff accountable when student data are inappropriately used or shared.
- To be most effective, staff training will include context-relevant examples of appropriate and inappropriate data use and sharing.

Action Steps

- ✓ Review your district's policy for data use by school officials.
- ✓ Review your district's training program on data use and student privacy.
- ✓ See the Model Notification of Rights under FERPA for Elementary and Secondary Schools, prepared by the U.S. Department of Education's Family Policy Compliance office, available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html
- ✓ See the FERPA training materials available from PTAC at http://ptac.ed.gov/toolkit_legal_references

Related Case Studies

Case studies #5, #6, #8, and #9 also pertain to appropriate sharing of data among instructional staff.

Case Study #8: Sharing Student Data With Student Assistants and Parent Volunteers

Students and parents sometimes serve as tutors or office volunteers within a school. In some instances, these individuals may need access to data about individual students. This case study looks at how districts may choose to enable or restrict access to student data by students and parents who are providing instructional or administrative support within the school.

Scenario

Mr. Garcia, a high school science teacher, uses peer tutors (i.e., students within the school) to tutor his students who need assistance in mastering specific science concepts. The peer tutors are allowed to see the graded tests of the students with whom they are working so that they know where assistance is needed. Meanwhile, Ms. Carroll, the school secretary, is using co-op students (students on a work-study program) to catch up on data entry tasks involving student data. Since the peer tutors and co-op students are being given access to the data for legitimate educational or official purposes, neither Mr. Garcia or Ms. Carroll see any problem in allowing students access to data about other students in the school.

FERPA School Official Exception

FERPA allows student data to be shared with anyone considered a school official who needs to access a student's data for educational purposes. Districts vary in how they define "school official," as well as the amount of student data to which individual school officials have access. The district's annual notification to parents and eligible students regarding their rights under FERPA should be used to explain how the district defines school official.

Best Practice Challenge

How does a district allow students or parents who are providing instructional or administrative support to access student data without violating student privacy requirements or ethics?

District Practices

- Some districts choose not to allow students to work in any situation where they are given access to student data, even though it may technically be legal to do so.
- Co-op students assigned to work in the school office can be given non-sensitive duties so that office staff are free to handle data entry responsibilities.
- Some districts require any volunteer or co-op student who may have access to student data to undergo the same kind of training required of staff who are given access to student data. In some cases, the districts require affidavits of nondisclosure from any individual 18 or older who is given access to student data.
- The annual FERPA notification to parents is used to identify school officials who will be given access to student data as needed, such as teachers, counselors, student teachers, substitute teachers, peer tutors, volunteer tutors, etc.

Lessons Learned

- All district staff, including teachers, must be trained on state and local restrictions regarding student access to other students' data.
- When generic training modules are used (e.g., PTAC, or state-developed modules), districts may have a challenge in certifying who has completed training. Options for obtaining certification include using an online "I Certify" program (or Survey Monkey or Google Forms), or have staff sign hard-copy affidavits.

Action Steps

- ✓ Review your district's policy for data use by school officials.
- ✓ Review your district's training program on data use and student privacy.
- ✓ See the Model Notification of Rights under FERPA for Elementary and Secondary Schools, prepared by the U.S. Department of Education's Family Policy Compliance office, available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html.
- ✓ See the FERPA training materials available from PTAC at http://ptac.ed.gov/toolkit_legal_references.

Related Case Studies

Case studies #5, #6, #7, and #9 also pertain to appropriate sharing of data among instructional staff.

Case Study #9: Sharing Student Data With Substitute Teachers

Substitute teachers are used in almost every school. They are generally considered school officials, but districts vary in the extent to which they give substitutes access to student data. This case study looks at how substitute teachers can securely access the data they need to do their jobs.

Scenario

Ms. Taylor is a new middle school math teacher. She needs to take personal leave the following day, and she knows her substitute teacher will need access to her student's information in order to assign them to appropriate test review groups and take attendance for the day. She starts to write out her log-in name and password so the substitute can access the system, but she recalls hearing in her data system training that she should never share her log-in information under any circumstance. She decides to ask the school secretary how she is supposed to provide access to the data system for her substitute teachers.

FERPA School Official Exception

FERPA allows student data to be shared with anyone considered a school official who needs to access a student's data for educational purposes. Districts vary in how they define "school official," as well as the amount of student data to which individual school officials have access. The district's annual notification to parents and eligible students regarding their rights under FERPA should be used to explain how the district defines school official.

Best Practice Challenge

How can districts provide substitute teachers with access to the specific student data they need for the limited amount of time they may be in the classroom?

District Practices

- All approved substitutes must go through training and sign affidavits that they understand the restrictions on the use and sharing of student data.
- In some districts, short-term substitutes are not given access to the data system. In those cases, the teacher of record must provide the substitute with the information they need to provide instruction. The substitute takes attendance manually and provides the information to office staff who enter it into the data system. Long-term substitutes are entered into the system as teacher-of-record for the class until the regular teacher returns. The long-term substitute then has the same access to the system as the regular teacher would have, using his or her own log-in name and password. By using individual log-in accounts for the long-term substitutes, an audit trail is created to determine who has been accessing the data and making any changes.
- Some districts provide access to the data system for all substitute teachers, regardless of the length of their assignment. When a substitute is assigned to a class, they are given access to the regular teacher's student data using their own log-in name and password.
- In some districts, staff at the individual buildings are responsible for creating accounts within the student information system for substitute teachers.
- Substitutes can be listed in a district's annual FERPA notification to parents. Substitute and student teachers are generally considered to be valid school officials.

Lessons Learned

- In districts where substitutes are given open access to the data system until district staff are informed of their departure, it is important that the IT department be informed when the regular classroom teacher has returned so that the substitute's access can be terminated until he or she has a new assignment.

Action Steps

- ✓ Review your district's policy for data use by school officials.
- ✓ Review your district's training program on data use and student privacy.
- ✓ See the Model Notification of Rights under FERPA for Elementary and Secondary Schools, prepared by the U.S. Department of Education's Family Policy Compliance office, available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html.
- ✓ See the FERPA training materials available from PTAC at http://ptac.ed.gov/toolkit_legal_references.

Related Case Studies

Case studies #5, #6, #7, and #8 also pertain to appropriate sharing of data among instructional staff.

Case Study #10: Data Sharing Among Community Schools and Community-based Organizations

Community schools offer at-risk students a variety of public services coordinated through a single site. Typically, various education and health services are offered through community schools, and a variety of community organizations may offer programs at the school. The sometimes complex inter-relationships among participating organizations in a community school can present challenges in appropriately sharing and protecting student data among the organizations. However, there are a number of scenarios under which the data sharing would be allowed under FERPA. Community schools must also be mindful of state and local laws that govern the sharing of data. This case study examines how community schools can share data with partner organizations to support the education and well-being of its students.

Scenario

Forest Hills High School is a community school that offers education, health, and social services to its students. The school's goal is to improve student achievement by fostering other aspects of the student's development—such as social, emotional, and physical health—that are needed to ensure students attend school ready to learn. In order to best serve its students and their parents, the school determines that it needs to share information about students with other community organizations. Forest Hills is the first community school in the district, and there are no formal processes in place yet for data sharing.

Best Practice Challenge

How can community schools share student-level data with other community organizations while protecting the privacy of the individual and adhering to federal and state privacy laws?

District Practices

One district has found that most of the community-based organizations with which they partner in their community schools offer services that fall under FERPA's school official exception. This would apply to organizations that are under contract with the district to provide services to students on behalf of the school, or provide services directly to the school. If an organization does not fall under the school official exception, then the district obtains parental consent for the school to share data with the partner organization as needed. If an organization is providing research services, other exceptions apply and a memorandum of understanding (MOU) is needed in accordance with both the studies exception and the audit or evaluation exception under FERPA. The parental consent requests and the MOU clearly state that the data are used for educational purposes. When aggregate data are needed for reports to funders, the district provides de-identified data to the partner organizations to conduct the analysis and prepare the report.

Lessons Learned

- To be successful, regular communications and documentation are needed between the school and its partner organizations.
- Some partner organizations in community schools need to report student outcomes to their funders. The school needs to take care in (1) providing aggregate data to donors that are appropriately suppressed to prevent identifying individual students, and (2) reviewing the claims that the organizations are making to be sure the data support those claims.

- Some districts facilitate information sharing on students with social service agencies outside of community schools in order to make sure all students get the assistance they need. The basis for these types of partnerships is strong memoranda of understanding.

Action Steps

- ✓ Review the FERPA exceptions that may allow for data sharing among partner organizations. See PTAC's FERPA Exceptions Summary available at http://ptac.ed.gov/ferpa-exceptions-summary-toolkit.
- ✓ Districts with community schools may want to consider establishing an interagency data governance council to coordinate the sharing of student-level data.
- ✓ See the SLDS best practice brief on P20W Data Governance available from NCES at http://nces.ed.gov/programs/slds/pdf/brief4_P_20W_DG.pdf.
- ✓ Although the publication is intended for interagency data sharing at the state level, many of the tips may be helpful in organizing data governance structures among local organizations and agencies.
- ✓ Review The Family Educational Rights and Privacy Act Guidance on Sharing Information with Community-Based Organizations published by the U.S. Department of Education's Family Policy Compliance Office and available at https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-and-community-based-orgs.pdf.

Related Case Studies

Case study #5 includes information on preventing disclosures of student PII in aggregate reports that may be used in community schools.

Case Study #11: Use of Social Media

Most school districts include student photographs as designated directory information. However, new social media are complicating the issue of how and when student images can be used. One concern is ensuring that any student whose parents opted out of sharing directory information is not included in images shared via social media by the school. This case study looks at how schools can protect student privacy when using social media to livestream school events.

Scenario

Madison High School wants to encourage parental engagement through the use of Facebook and Twitter. The school decides to livestream a student concert so that parents who cannot attend in person can virtually participate in the event. The school includes photos as part of its official directory information, but school staff failed to check for opt-outs before streaming the concert. Sally Cook is one of the student musicians who performed in the concert. Sally is currently living with a foster family because her own parents, who live in a nearby school district, have been deemed by the court to be a potential danger to her. When her foster mother finds out the school has livestreamed an event in which Sally participated, she complains to the principal that the school has endangered Sally by making the video available on social media where it might be accessed by others. She points out that she specifically opted out of sharing Sally's photo in school publications or other communications.

Best Practice Challenge

How can schools use social media to engage parents without violating student privacy?

District Practices

- Some districts include a media release for parents to sign in the back-to-school paperwork. It requests permission to use voice or video images of the student in various school communications, including social media. It goes beyond the standard photo release that may be part of the annual FERPA notification and opt-out process.
- One district advises staff to only show faces of students for whom the districts have received parental approval. The faces of other students can be distorted to protect their identity.
- Some districts record the opt-out status for the use of a student's voice or image in the student management system. The system includes a canned report so users can easily identify the opt-out status of parents at the school or district levels.

Lessons Learned

- Electronic communications make it difficult to set boundaries; they can easily be copied and shared with others. Thus, it is particularly important that schools follow all district guidelines for the use of social media.
- When possible, film from angles so student faces are not clearly visible.
- At the high school level, if students are told they will be on camera at a school event, they will likely take steps to avoid being filmed if needed.
- School districts are generally not responsible for the actions of parents who post pictures or videos of school events on their personal websites. School districts are responsible for the pictures of videos they produce and maintain.

Action Steps

- ✓ Review the district's directory information policy and/or standard media release to determine the use of student images in publications or social media is covered.
- ✓ Include the use of social media in annual training sessions with staff.

Related Case Studies

Case studies #3 and #4 also pertain to the sharing of directory information. See the section on Federal Laws in Chapter One for an overview of directory information policies under FERPA.

Appendix A. References Used in Preparing This Document

Access 4 Learning Community (A4L 2015.) Press release "Student Data Privacy Consortium launched to support 'frontline' education stakeholders," issued December 9, 2015. Retrieved February 10, 2016 from https://www.sifassociation.org/NewsRoom/Press%20Releases/Student%20Data%20Privacy%20Consortium%20launched%20to%20support%20front%20line%20education%20stakeholders.pdf.

California Legislative Information (CLI 2014). Senate Bill 1177. Retrieved February 10, 2016 from https://leginfo. legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177.

Congress.gov (2015). *H.R.2092 - Student Digital Privacy and Parental Rights Act of 2015*, April 29, 2015. Retrieved October 5, 2015 from https://www.congress.gov/bill/114th-congress/house-bill/2092.

Council of Chief State School Officers (CCSSO 2014). *CA Signs Into Law the Student Online Personal Protection Act (SOPIPA)* (online news brief). Monday, October 6, 2014. Retrieved October 5, 2015 from http://www.ccsso.org/News_and_Events/Current_News/CA_Signs_Into_Law_the_Student_Online_Personal_Information_Protection_Act_(SOPIPA)_.html downloaded October 5, 2015.

Data Quality Campaign (DQC 2015). *Student Data Privacy Legislation: What Happened in 2015, and What's Next*. Washington, DC: Author. Retrieved May 19, 2016, from http://dataqualitycampaign.org/resource/student-data-privacy-legislation-happened-2015-next/

Data Quality Campaign (DQC 2011). *U.S. Department of Education Final FERPA Regulations: Advisory and Overview*, prepared by Education Counsel LLC. Washington, DC: Author. Retrieved May 19, 2016 from http://dataqualitycampaign.org/resource/u-s-department-education-final-ferpa-regulations-advisory-overview/

Family Policy and Compliance Office of the U.S. Department of Education (FPCO 2004). *Legislative History of Major FERPA Provisions*. Retrieved November 9, 2015 from http://www2.ed.gov/print/policy/gen/guid/fpco/ferpa/leg-history.html.

Family Policy and Compliance Office of the U.S. Department of Education (FPCO 2008). *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) And the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records.* Retrieved February 10, 2016 from http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf.

Family Policy and Compliance Office of the U.S. Department of Education (FPCO 2002). *Policy Guidance - Access to High School Students and Information on Students by Military Recruiters*. Retrieved November 9, 2015 from http://www2.ed.gov/policy/gen/guid/fpco/hottopics/ht-10-09-02a.html.

Federal Trade Commission (FTC 2015). *Complying with COPPA: Frequently Asked Questions*. Retrieved December 15, 2015 from https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

Federal Trade Commission (FTC 2016). *Consumer Information* webpage. Retrieved March 5, 2016 from https://www. consumer.ftc.gov/articles/0003-phishing.

Future of Privacy Forum (FPF 2015). *Beyond the Fear Factor: Parental Support for Technology and Data Use in Schools*. Washington, DC: Author. Retrieved May 19, 2016 from https://fpf.org/2015/09/25/13215/

Herold, Benjamin and Lauren Camera (2015). “Educators Hope Congress Provides Clarity, Support on Privacy Issues,” *Education Week*, October 21, 2015. Retrieved October 21, 2015 from http://www.edweek.org/ew/articles/2015/10/21/educators-hope-congress-provides-clarity-support-on.html?cmp=eml-eb-sr-data+102115.

Kamisar, Ben (2014). “InBloom Sputters as Data Privacy Hits Spotlight,” *Education Week*, January 8, 2014. Retrieved October 5, 2015 from http://www.edweek.org/ew/articles/2014/01/08/15inbloom_ep.h33.html?r=182194026.

Louisiana Department of Education (2015). *Louisiana’s Plan to Protect Student Privacy*. November 2015. Retrieved December 11, 2015 from http://www.louisianabelieves.com/docs/default-source/data-management/2015-student-privacy-planning-guide-(web).pdf?sfvrsn=6.

National Center for Education Statistics (NCES 2012). *P-20 Data Governance: Tips from the States,* SLDS Best Practices Brief 4. Washington DC: Author. Retrieved October 5, 2015 from https://nces.ed.gov/programs/slds/pdf/brief4_P_20W_ DG.pdf.

National Forum on Education Statistics (NFES 2010). *Traveling Through Time: The Forum Guide to Longitudinal Data Systems Part 2: Planning and Developing an LDS*. Washington, DC: National Center for Education Statistics, Institute of Education Sciences, U.S. Department of Education. Retrieved October 14, 2015 from http://nces.ed.gov/forum/pub_2011804.asp.

North Dakota State Government, *Senate Bill No. 2326*. Retrieved November 10, 2015 from http://www.legis.nd.gov/assembly/64-2015/documents/15-0956-05000.pdf?20151110150311.

Oklahoma State Department of Education (OKSDE 2015). *Data Privacy and Security*. Retrieved October 5, 2015 from http://ok.gov/sde/data-privacy-and-security.

Privacy Technical Assistance Center of the U.S. Department of Education (PTAC 2015-a). *Data Governance and Stewardship*. Retrieved October 5, 2015 from http://ptac.ed.gov/sites/default/files/Data_Governance_and_Stewardship.pdf.

Privacy Technical Assistance Center (PTAC 2015-b). *Data Governance Checklist.* Retrieved October 5, 2015 from http://ptac.ed.gov/sites/default/files/Data%20Governance%20Checklist%20%281%29.pdf.

Privacy Technical Assistance Center (PTAC 2015-c). *Data Security Checklist.* Retrieved October 5, 2015 from http://ptac.ed.gov/sites/default/files/Data%20Security%20Checklist.pdf.

Privacy Technical Assistance Center (PTAC 2015-d). *Developing a Privacy Program for Your District.* Retrieved February 10, 2016 from http://ptac.ed.gov/ptac-guidance-videos.

Washington State Legislature, *Enacting the Student User Privacy in Education Rights Act*. Retrieved December 15, 2015 from http://app.leg.wa.gov/billinfo/summary.aspx?year=2015&bill=5419.

Appendix B. Resources on Education Data Privacy

The following is a sample list of resources related to the protection of education data privacy. This list is not intended to be comprehensive. Privacy is emerging as a critical issue in today's society, and many organizations are offering helpful resources on privacy protection.

FEDERAL RESOURCES

U.S. Department of Agriculture

- Food and Nutrition Services (FNS)

The FNS administers the National School Lunch Program and provides official guidance on protecting the confidentiality of free- and reduced-price lunch eligibility status of students. In particular, see Chapter 5: Confidentiality and Disclosure of the 2015 edition of the *Eligibility Manual for School Meals. Determining and Verifying Eligibility,* published by the U.S. Department of Agriculture, Food and Nutrition Service. http://www.fns.usda.gov/sites/default/files/cn/SP40_CACFP18_SFSP20-2015a.pdf.

U.S. Department of Commerce

- Federal Trade Commission (FTC)

The FTC is responsible for regulating and enforcing the provisions of the Children's Online Privacy Protection Act (COPPA). COPPA generally applies only to commercial (for-profit) vendors. See *Complying with COPPA: Frequently Asked Questions*, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

U.S. Department of Education

- Family Policy and Compliance Office (FPCO)

The mission of the FPCO is to effectively implement two laws that seek to ensure student and parental privacy rights in education: the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA). FPCO offers a number of guidance documents related to education privacy. For more information, visit http://www2.ed.gov/policy/gen/guid/fpco/index.html.

- National Center for Education Statistics (NCES)

NCES has developed several technical briefs to assist states with protecting the privacy and confidentiality of student data:

  - *Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records* (2010) http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011601
  - *Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records* (2010) http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602
  - *Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting* (2010) http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011603

In addition, NCES's National Forum on Education Statistics (Forum) has published resources for state and local education agencies related to the protection of student privacy, as well as other important topics regarding the use of education data. For a full listing of Forum publications, see http://nces.ed.gov/forum/publications.asp.

- Privacy Technical Assistance Center (PTAC)

PTAC was established to assist education agencies, school officials, teachers, parents, and other education stakeholders in understanding and implementing the requirements of the Family Educational Rights and Privacy Act. PTAC offers a variety of resources related to student data and student data systems, including publications, training materials, and technical assistance. See http://ptac.ed.gov.

STATE RESOURCES

Increasingly, state education agencies and state education professional groups are publishing information related to the protection of education data on their websites. Listed below are examples of the types of resources available from state organizations and agencies.

The **California Education Technology Professional Association**, in collaboration with the California County Superintendents Educational Services Association and the Fagen, Friedman and Fulfrost law firm, developed a *Data Privacy Guide* and an *Ask Before You App* video to help teachers and administrators understand state and federal legal privacy requirements. The resources can be downloaded from http://www.f3law.com/foundation.php?id=155.

Colorado's guidance document for districts on privacy and security can be found at https://www.cde.state.co.us/cdereval/districtguidanceoninformationsecurityandprivacypolicies.

The **Massachusetts Student Privacy Alliance** offers model agreements and a sample application database at https://secure2.cpsd.us/mspa/index.php. (See also the MSPA Student Data/Data Breach Special Terms and Conditions form in Appendix C.)

The **New York** State Regional Information Center on Data Security & Privacy can be found at http://nysdsp.org/.

The **West Virginia** Department of Education's Data Access and Management Guidance can be found at http://static.k12.wv.us/tt/2014/datamanagement_guidance%20FINAL%201-21-14.pdf; the training menu for LEAs can be found at http://wvde.state.wv.us/forms/zoomwv/zoomwv_trainingmenu.pdf.

NONPROFIT ORGANIZATIONS

The following nonprofit organizations are examples of groups that provide resources related to education data privacy.
Access 4 Learning. Formerly the SIF Association, Access 4 Learning is a global community focused on education data and information technology. Its members include education policymakers and practitioners as well as education technology service providers. Access 4 Learning supports collaborative efforts among its members. For more information, see https://www.sifassociation.org/Pages/default.aspx.

Common Sense Media. A nonprofit organization dedicated to helping parents and children safely use media and technology. For more information, see https://www.commonsensemedia.org/about-us/our-mission#about-us.

Consortium for School Networking (CoSN). A professional association for school district technology leaders, CoSN offers a *Protecting Student Privacy in Connected Learning Toolkit*. This resource is available for free download at http://cosn.org/. Note, however, that you must first create a log-in account in order to access the online store. In addition, CoSN has developed a "Trusted Learning Environment" seal for schools. For more information, see http://trustedlearning.org.

Data Quality Campaign. A national, nonprofit organization that provides free resources related to the effective and appropriate use of student data. One of DQC's key action areas is Privacy, Security, and Confidentiality. For more information, see http://dataqualitycampaign.org.

Future of Privacy Forum. A Washington, DC-based think tank that seeks to advance responsible data practices across various sectors, including education. The Forum publishes white papers and other resources that highlight emerging trends in privacy protection. For more information, see https://fpf.org.

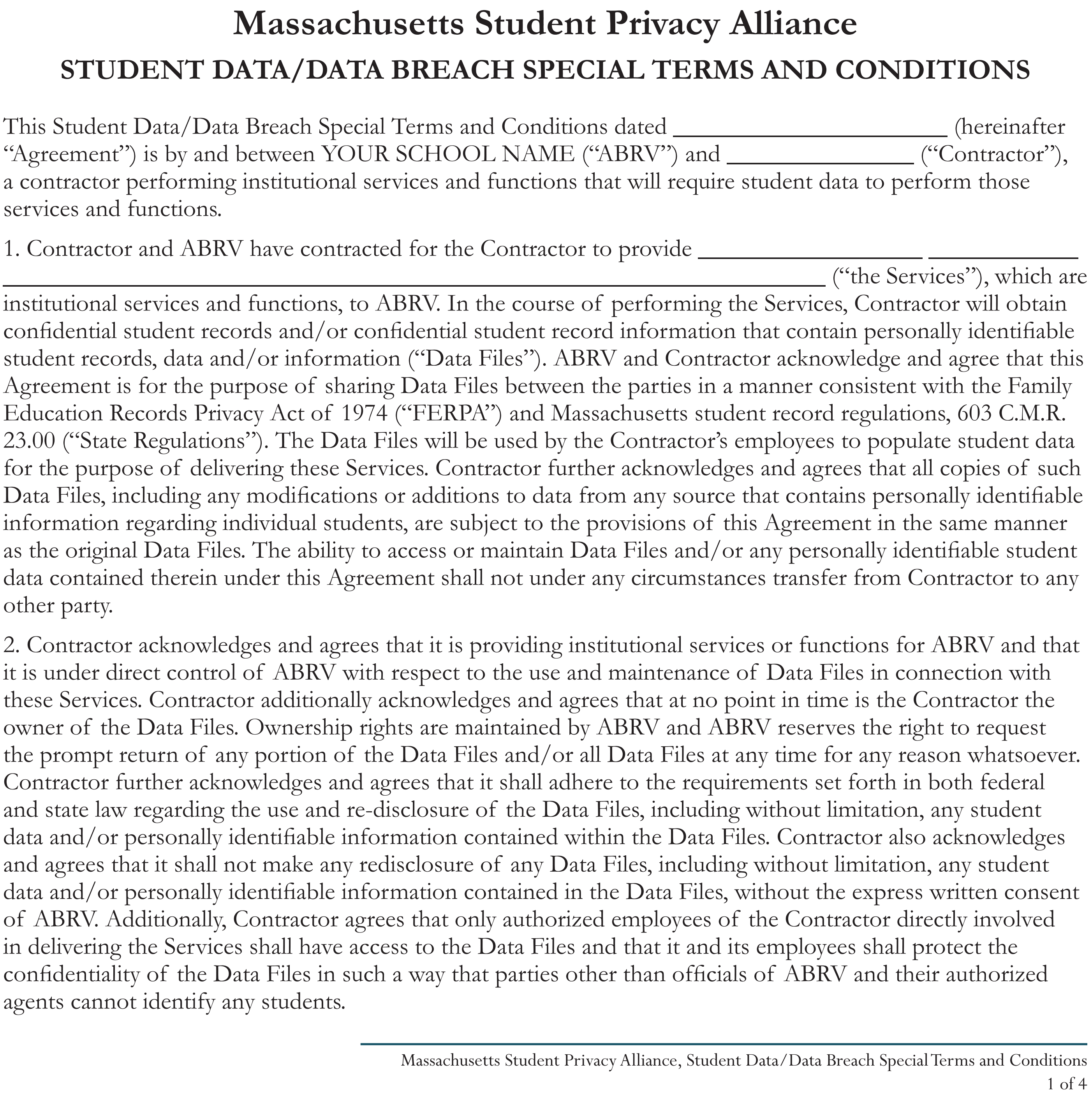
iKeepSafe.ORG. The Internet Keep Safe Coalition (iKeepSafe) is a nonprofit international alliance of more than 100 policy leaders, educators, law enforcement members, technology experts, public health experts, and advocates. The group tracks global trends and issues surrounding digitally connected products and their impact on children. For more information, see http://ikeepsafe.org/about-us/.

National Cyber Security Alliance. This organization sponsors the Stay Safe Online initiative, which provides training to raise awareness about how people can protect their personal information online. They also sponsor Data Privacy Day. For more information, see www.staysafeonline.org.

National Institute of Standards and Technology. Part of the U.S. Department of Commerce, NIST houses a computer security resource center offering free security resources. For more information, see http://csrc.nist.gov/.

Appendix C. Sample Documents

The documents included in this appendix were current as of the date that they were downloaded. Many privacy-related documents are "works in progress," as privacy law evolves and methods for managing new technologies are developed. These sample documents have not been evaluated for compliance with any state or federal laws. They are provided simply as examples of privacy-related forms and guidance.



Massachusetts Student Privacy Alliance

STUDENT DATA/DATA BREACH SPECIAL TERMS AND CONDITIONS

This Student Data/Data Breach Special Terms and Conditions dated ______________________ (hereinafter "Agreement") is by and between YOUR SCHOOL NAME ("ABRV") and ________________ ("Contractor"), a contractor performing institutional services and functions that will require student data to perform those services and functions.

1. Contractor and ABRV have contracted for the Contractor to provide ____________________ _____________ ____ ("the Services"), which are institutional services and functions, to ABRV. In the course of performing the Services, Contractor will obtain confidential student records and/or confidential student record information that contain personally identifiable student records, data and/or information ("Data Files"). ABRV and Contractor acknowledge and agree that this Agreement is for the purpose of sharing Data Files between the parties in a manner consistent with the Family Education Records Privacy Act of 1974 ("FERPA") and Massachusetts student record regulations, 603 C.M.R. 23.00 ("State Regulations"). The Data Files will be used by the Contractor's employees to populate student data for the purpose of delivering these Services. Contractor further acknowledges and agrees that all copies of such Data Files, including any modifications or additions to data from any source that contains personally identifiable information regarding individual students, are subject to the provisions of this Agreement in the same manner as the original Data Files. The ability to access or maintain Data Files and/or any personally identifiable student data contained therein under this Agreement shall not under any circumstances transfer from Contractor to any other party.

2. Contractor acknowledges and agrees that it is providing institutional services or functions for ABRV and that it is under direct control of ABRV with respect to the use and maintenance of Data Files in connection with these Services. Contractor additionally acknowledges and agrees that at no point in time is the Contractor the owner of the Data Files. Ownership rights are maintained by ABRV and ABRV reserves the right to request the prompt return of any portion of the Data Files and/or all Data Files at any time for any reason whatsoever. Contractor further acknowledges and agrees that it shall adhere to the requirements set forth in both federal and state law regarding the use and re-disclosure of the Data Files, including without limitation, any student data and/or personally identifiable information contained within the Data Files. Contractor also acknowledges and agrees that it shall not make any redisclosure of any Data Files, including without limitation, any student data and/or personally identifiable information contained in the Data Files, without the express written consent of ABRV. Additionally, Contractor agrees that only authorized employees of the Contractor directly involved in delivering the Services shall have access to the Data Files and that it and its employees shall protect the confidentiality of the Data Files in such a way that parties other than officials of ABRV and their authorized agents cannot identify any students.

3. Contractor also acknowledges and agrees to:

(i) use personally identifiable student data shared under this Agreement for no purpose other than in connection with and through the provision of the Services.

(ii) use reasonable methods, consistent with industry standards, to protect the Data Files and/or any personally identifiable student data contained therein from redisclosure, and to not share the Data Files and/or any personally identifiable student data received under this Agreement with any other entity without prior written approval from ABRV.

(iii) not copy, reproduce or transmit the Data Files and/or any personally identifiable student data contained therein ,except as necessary to fulfill the Services.

(iv) notify the Chief Information Officer for ABRV in writing within three (3) days of its determination that it has experienced a data breach, breach of security or unauthorized acquisition or use of any Data Files and/or personally identifiable student data contained therein. Contractor agrees that said notification shall include, to the extent feasible, the date or approximate dates of such incident and the nature thereof, the specific scope of said breach (i.e., what data was accessed, used, released or otherwise breached, including the names of individual students that were affected by said breach) and what actions or steps with respect to the incident that Contractor plans to take or has taken in response to said breach.

(v) not provide any Data Files or any personally identifiable data contained therein to any party ineligible to receive student records and/or student record data and information protected by FERPA and State Regulations or prohibited from receiving personally identifiable from any entity under 34 CFR 99.31(a)(6)(iii).

(vi) to maintain backup copies, backed up at least daily, of Data Files in case of Contractor system failure or any other unforeseen event resulting in loss of Data Files.

(vii) to, upon receipt of a request from ABRV, immediately provide ABRV with any specified portion of the Data Files within three (3) days of receipt of said request

(viii) to, upon receipt of a request from ABRV, immediately begin the process of returning all Data Files over to ABRV and subsequently erasing and/or otherwise destroying any Data Files, be it digital or physical form, still in Contractor's possession such that Contractor is no longer in possession of any student work belonging to ABRV and to provide ABRV with any and all Data Files in Contractor's possession, custody or control within seven (7) days of receipt of said request.

(ix) to, in the event of the Contractor's cessation of operations, promptly return all Data Files to ABRV in an organized, manageable manner and subsequently erasing and/or otherwise destroying any Data Files, be it digital or physical form, still in Contractor's possession such that Contractor is no longer in possession of any student work belonging to ABRV.

(x) to delete ABRV Data Files that it collects or receives under this Agreement once the Services referenced in this Agreement lapses.

(xi) to, upon receipt of a litigation hold request from ABRV, immediately implement a litigation hold and preserve all documents and data relevant identified by ABRV and suspend deletion, overwriting, or any other possible destruction of documentation and data identified in, related to, arising out of and/or relevant to the litigation hold.

4. Contractor certifies under the penalties of perjury that it complies with all federal and state laws, regulations and rules as such laws may apply to the receipt, storing, maintenance or access to personal information, including without limitation, all standards for the protection of personal information of residents of the Commonwealth and maintaining safeguards for personal information. Contractor hereby further certifies under penalties of perjury that it has a written comprehensive information security program that is in compliance with the provisions of 201 C.M.R. 17.00 et seq. Further, the Contractor hereby certifies under the penalties of perjury that it shall fully comply with the provisions of the federal Family Educational Rights Privacy Act, 20 U.S.C. §1232g and regulations promulgated thereunder and Massachusetts student records law and regulations, including without limitation, 603 C.M.R. 23.00 et seq., and to fully protect the confidentiality of any student data and/or personally identifiable information provided to it or its representatives. Contractor further represents and warrants that it has reviewed and complied with all information security programs, plans, guidelines, standards and policies that apply to the work it will be performing, that it will communicate these provisions to and enforce them against its subcontractors and will implement and maintain any other reasonable and appropriate security procedures and practices necessary to protect personal information and/or student record information from unauthorized access, destruction, use, modification, disclosure or loss. Contractor also represents and warrants that if personal information and/or student record information is to be stored on a laptop or other mobile electronic device, that such electronic devices are encrypted and that all such devices will be scanned at the completion of any contract or service agreement and/or research study or project to ensure that no personal information and/or student record information is stored on such electronic devices. Furthermore, Contractor represents and warrants that it has in place a service that will allow it to wipe the hard drive on any stolen laptop or mobile electronic device remotely and have purchased locks for all laptops and mobile electronic devices and have a protocol in place to ensure use by employees.

5. Contractor represents, warrants and agrees that its terms of service/terms and conditions of use and/or privacy policies dated _________________shall be amended as it relates to the Services as follows:

a. Any indemnification provision contained in the Contractor's terms of service, terms and conditions of use and/or privacy policies are hereby deleted in their entirety.

b. Any provision in the Contractor's terms of service, terms and conditions of use and/or privacy policies that require that the City and/or ABRV, as a user, to carry insurance coverage are hereby deleted in their entirety.

c. Any provision in the Contractor's terms of service, terms and conditions of use and/or privacy policies which specifically disclaim all implied warranties or merchantability, non-infringement and fitness for a particular purpose, the implied conditions of satisfactory quality and acceptance as well as any local jurisdictional analogues to the above and other implied or statutory warranties are hereby deleted in its entirety.

d. Any provision in the Contractor's terms of service, terms and conditions of use and/or privacy policies by which the City and/or ABRV is specifically releasing the Contractor from liability are hereby deleted in their entirety.

e. Any changes that the Contractor may make, from time to time, to its terms of service, terms and conditions of use and/or privacy policies, shall not apply to the terms of these Services unless the Contractor and City and/or ABRV agree to such changes in writing.

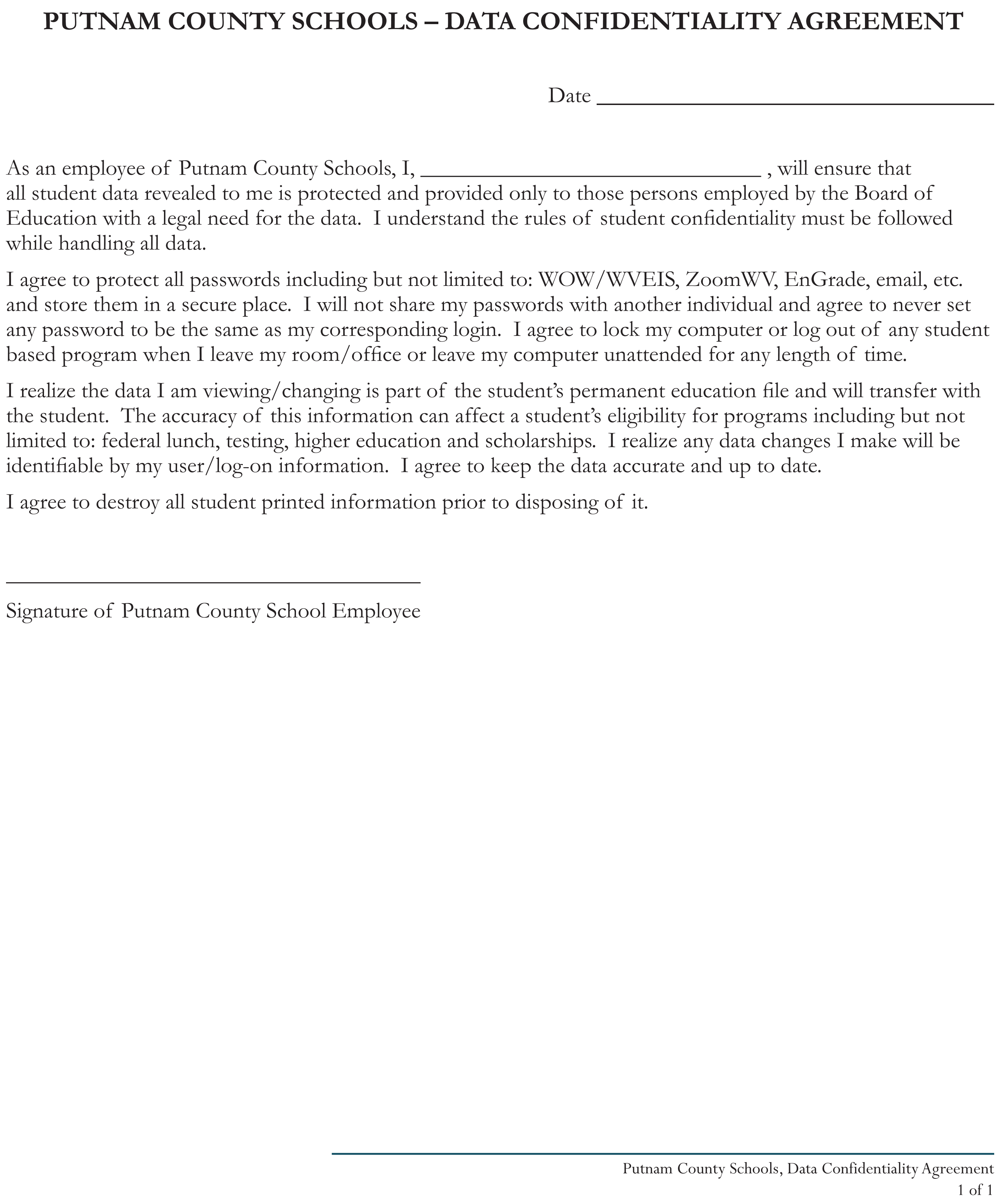
f. The laws of the Commonwealth of Massachusetts shall govern this Agreement and the Governing Law provision of the Contractor's terms of service, terms and conditions of use and license agreement and/or privacy policies are hereby deleted in their entirety.

6. Contractor represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Data Files and any personally identifiable student data contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data Files and/or any personally identifiable student data contained therein, or may own, lease or control equipment or facilities of any kind where the Data Files and any personally identifiable student data contained therein is stored, maintained or used in any way.

IN WITNESS WHEREOF, and in consideration of the mutual covenants set forth herein and for other good and valuable consideration, and intending to be legally bound, each party has caused this Agreement to be duly executed as a Massachusetts instrument under seal as of the day and year first written above.

INSERT NAME OF CONTRACTOR	*YOUR SCHOOL NAME*
______________________________	______________________________
Name	Superintendent of Schools
______________________________	
Title	

Massachusetts Student Privacy Alliance, Student Data/Data Breach Special Terms and Conditions
4 of 4



PUTNAM COUNTY SCHOOLS – DATA CONFIDENTIALITY AGREEMENT

Date ______________________________

As an employee of Putnam County Schools, I, _________________________ , will ensure that all student data revealed to me is protected and provided only to those persons employed by the Board of Education with a legal need for the data. I understand the rules of student confidentiality must be followed while handling all data.

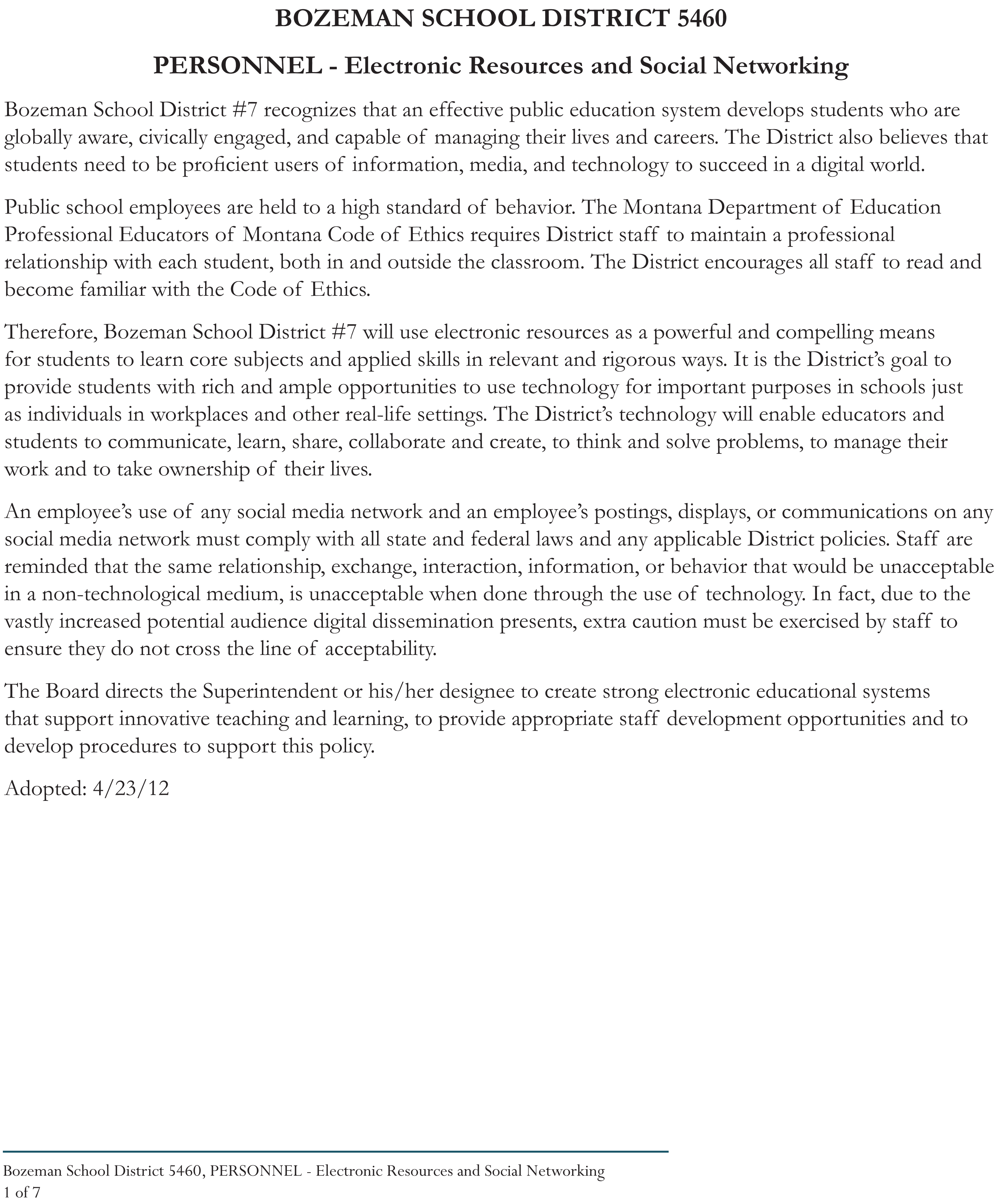
I agree to protect all passwords including but not limited to: WOW/WVEIS, ZoomWV, EnGrade, email, etc. and store them in a secure place. I will not share my passwords with another individual and agree to never set any password to be the same as my corresponding login. I agree to lock my computer or log out of any student based program when I leave my room/office or leave my computer unattended for any length of time.

I realize the data I am viewing/changing is part of the student's permanent education file and will transfer with the student. The accuracy of this information can affect a student's eligibility for programs including but not limited to: federal lunch, testing, higher education and scholarships. I realize any data changes I make will be identifiable by my user/log-on information. I agree to keep the data accurate and up to date.

I agree to destroy all student printed information prior to disposing of it.

____

Signature of Putnam County School Employee



BOZEMAN SCHOOL DISTRICT 5460

PERSONNEL - Electronic Resources and Social Networking

Bozeman School District #7 recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The District also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Public school employees are held to a high standard of behavior. The Montana Department of Education Professional Educators of Montana Code of Ethics requires District staff to maintain a professional relationship with each student, both in and outside the classroom. The District encourages all staff to read and become familiar with the Code of Ethics.

Therefore, Bozeman School District #7 will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the District's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings. The District's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work and to take ownership of their lives.

An employee's use of any social media network and an employee's postings, displays, or communications on any social media network must comply with all state and federal laws and any applicable District policies. Staff are reminded that the same relationship, exchange, interaction, information, or behavior that would be unacceptable in a non-technological medium, is unacceptable when done through the use of technology. In fact, due to the vastly increased potential audience digital dissemination presents, extra caution must be exercised by staff to ensure they do not cross the line of acceptability.

The Board directs the Superintendent or his/her designee to create strong electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities and to develop procedures to support this policy.

Adopted: 4/23/12

Sample Social Media Guidelines: Parent Permission Form for Student Participation

Dear Parent/Guardian:

This year, to help our students develop their ______________ skills as well as ___________________, students will use a variety of social media (apps, blogs, wikis, podcasts, etc.) via the Internet. Apps, social media and collaboration sites have become integral in the workplace and across college campuses. These activities support the District's vision to prepare students to succeed and make a difference in a rapidly changing world community.

Planned Activities:
Teacher provides description of activities, lists site(s)and indicates why specific parent permission is needed according to Terms of Service Agreement (if applicable) or release of Personally Identifiable Information.

I encourage you to learn more about the district's technology policies and procedures. Information may be found here (insert information sources). Projects may be shared privately with other classes over the Internet and with parents, and also may be shared publicly on the Internet. To protect student privacy and ensure safety throughout all projects we will: (1) Only use anonymous identifiers to identify student work and ideas; (2) Not use pictures of individual students; (3) Only use GROUP pictures of students which do not identify individuals by name if we share pictures of students working in class.

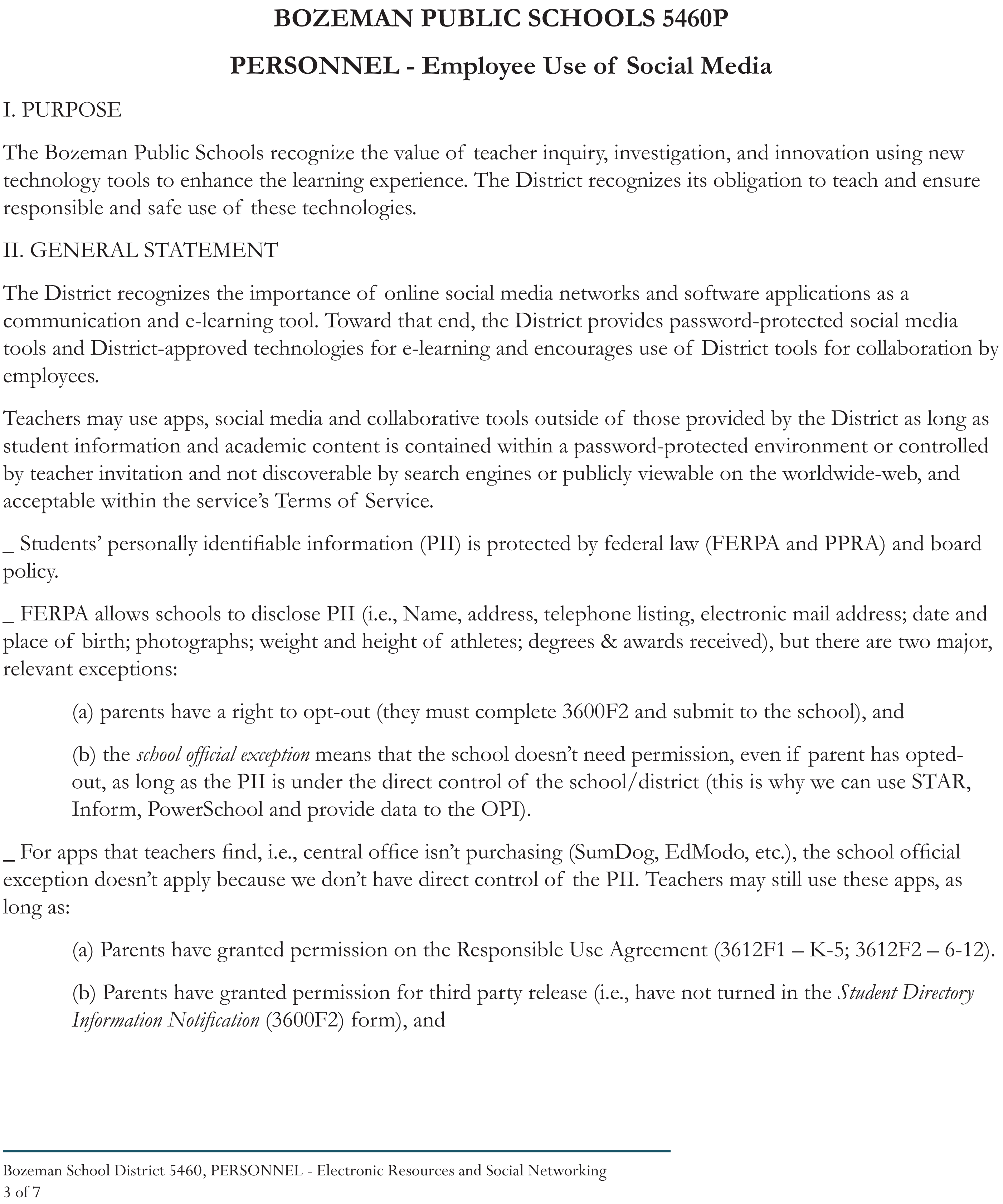
If you have questions or concerns about this/these projects, please contact me. If I'm not able to address your concerns, then we will work together to provide an alternate activity so that your child understands the content. I will be in contact with you to share links to specific projects as we create them! Please complete, sign and return the bottom of this form to me as soon as possible. Thanks!

_________ Yes, my child has my permission to participate in this teacher moderated, Internet--□ based apps/social media project(s) this year. [If Applicable – My child may share recordings on the Internet and participate in the planned collaborative activities outlined here.]

_________ No, my child does not have permission to participate in this/these activity/activities.

Student Name: _____________ Signature: __________________ Date:___________

Parent/Guardian Name: _________________ Signature: _____________ Date:___________



BOZEMAN PUBLIC SCHOOLS 5460P

PERSONNEL - Employee Use of Social Media

I. PURPOSE

The Bozeman Public Schools recognize the value of teacher inquiry, investigation, and innovation using new technology tools to enhance the learning experience. The District recognizes its obligation to teach and ensure responsible and safe use of these technologies.

II. GENERAL STATEMENT

The District recognizes the importance of online social media networks and software applications as a communication and e-learning tool. Toward that end, the District provides password-protected social media tools and District-approved technologies for e-learning and encourages use of District tools for collaboration by employees.

Teachers may use apps, social media and collaborative tools outside of those provided by the District as long as student information and academic content is contained within a password-protected environment or controlled by teacher invitation and not discoverable by search engines or publicly viewable on the worldwide-web, and acceptable within the service's Terms of Service.

_ Students' personally identifiable information (PII) is protected by federal law (FERPA and PPRA) and board policy.

_ FERPA allows schools to disclose PII (i.e., Name, address, telephone listing, electronic mail address; date and place of birth; photographs; weight and height of athletes; degrees & awards received), but there are two major, relevant exceptions:

> (a) parents have a right to opt-out (they must complete 3600F2 and submit to the school), and
>
> (b) the *school official exception* means that the school doesn't need permission, even if parent has opted-out, as long as the PII is under the direct control of the school/district (this is why we can use STAR, Inform, PowerSchool and provide data to the OPI).

_ For apps that teachers find, i.e., central office isn't purchasing (SumDog, EdModo, etc.), the school official exception doesn't apply because we don't have direct control of the PII. Teachers may still use these apps, as long as:

> (a) Parents have granted permission on the Responsible Use Agreement (3612F1 – K-5; 3612F2 – 6-12).
>
> (b) Parents have granted permission for third party release (i.e., have not turned in the *Student Directory Information Notification* (3600F2) form), and

(c) If parents have turned in the *Student Directory Information Notification (3600F2)* form (indicated in PowerSchool by a report titled *Permissions RUA,PII,FieldTrip*), parents have given express permission using *Apps/Social Media Guidelines: Parent Permission Form for Student Participation* (5460F) located in SchoolStream, and

(d) The teacher is following all of the Terms of Service (pay particular attention to age of use).

_ Steps teachers should follow to seek approval for (and possible purchase) an app to use in the classroom:

(a) Check PowerSchool to see if parents have granted permission on the Responsible Use Agreement (3612F1 – K-5; 3612F2 – 6-12).

(b) Student information and academic content are contained within a password-protected environment or controlled by teacher invitation and not discoverable by search engines or publicly viewable on the world-wide-web). Exceptions can be made for special circumstances. Teachers need principal and parental approval via *Apps/Social Media Guidelines: Parent Permission Form for Student Participation* (5460F) located on SchoolStream.

(c) Check the Terms of Service/Use and Privacy Policy of the resource. It is a contract and you, personally, are agreeing to the terms of the contract. Thus, if you instruct students 12 and under and the Terms of Service say it is for use by children 13 and older, you may not use it.

(d) Be very cautious of: Use of PII (e.g., Disclosure to Other Parties; ownership of student content). In these cases, please see your principal.

(e) Check PowerSchool to see if any families have signed a *Student Directory Information Notification* (3600F2). If they have, once your principal approves, you will have to have separate permission from those families using the *Apps/Social Media Guidelines: Parent Permission Form for Student Participation* (5460F) located on SchoolStream.

(f) Discuss with principal.

(g) Complete *Apps/Social Media Approval Form* on SchoolStream so that your principal is aware of the app/social media you are using and can provide final approval. It also helps you ensure that you are following the appropriate steps for parental permission.

(h) If purchasing apps for multiple iPads, submit the *Curriculum Support Request Form – iPad Apps Form* on SchoolStream.

_ Steps principals should follow:

(a) Ensure that teachers understand *privacy* and *terms of use* information.

(b) Know what is being used in your building. Teachers should go back and follow procedure if they have not gone through steps before. (Don't forget about PACs and Partner Organizations)

(c) Encourage your teachers to discuss a possible App/Terms of Service prior to *Apps/Social Media Approval Form* submittal on SchoolStream.

(d) Approve or disapprove the SchoolStream request. As the school administrator, you are the gatekeeper!

(e) If you have questions about Terms of Service or Privacy, contact the District's Technology Supervisor.

(f) Please note that response times may vary, as legal counsel may be required.

The line between professional and personal relationships is blurred within a social media context. When employees choose to join or engage with District students, families or fellow employees in a social media context that exists outside those approved by the District, they are advised to maintain their professionalism as District employees and have responsibility for addressing inappropriate behavior or activity on these networks, including requirements for mandated reporting.

III. DEFINITIONS

A. Social Media refers to a category of Internet-based tools that invite users to share and create content, often in a collaborative manner.

B. Apps/Applications refer to software program(s) designed to run on digital devices.

C. Public social media networks and collaborative tools are defined to include: web sites, web logs (blogs), social networks, online forums, and any other social media generally available to the public or consumers and which do not fall within the District's electronic technologies network.

D. District approved password-protected social media tools are those that fall within the District's electronic technologies network or which the District has approved for educational use. District approved social media tools limit public access.

IV. REQUIREMENTS

All employees are expected to serve as positive ambassadors for our schools and to remember they are role models to students in this community.

A. Employees may use their District e-mail address for communications on public social media networks for educational reasons.

B. Employees may not act as a spokesperson for the District or post comments as a representative of the District, except as authorized by the Superintendent or the Superintendent's designee.

C. Employees may not disclose information on any social media network that is confidential or proprietary to the District, its students, or employees or that is protected by data privacy laws.

D. Employees may not use or post the District logos on any social media network without permission from the Superintendent, or designee.

E. Employees may not post images of students on any social media network without written parental consent or verifying approval status from the Student Directory Information Notification form, except for images of students taken in the public arena, such as at sporting events or fine arts public performances.

F. The District and its employees have responsibility to protect minors from inappropriate content. District provided tools can limit public access and is easily monitored for inappropriate use. Employees who choose to use public social media networks for classroom purposes are expected to monitor student use and ensure that accessibility is limited to internal use only. If outside access is deemed necessary by the teacher, principal approval and formal, written parental consent are required.

G. Employees may not post floor plans of the District premises and property.

H. Employees have responsibility for maintaining appropriate employee-student relationships at all times and have responsibility for addressing inappropriate behavior or activity on any social network. This includes acting to protect the safety of minors online.

I. Employees who participate in social media networks may decide to include information about their work with the District as part of their personal profile, as it would relate to a typical social conversation. This may include work information included in a personal profile, to include District name, job title, and job duties; status updates regarding an employee's own job promotion; and personal participation in District-sponsored events, including volunteer activities.

V. GUIDELINES FOR SOCIAL MEDIA NETWORKS

These guidelines will continually evolve as new technologies and social networking tools emerge—so check back once in awhile to make sure you're up to date.

- It's your responsibility. What you write is ultimately your responsibility. If it seems inappropriate, use caution. Trademark, copyright, fair use and terms of use requirements must be respected.
- Ensure the safety of students. When employees, especially coaches/advisors, choose to join or engage with these social networking groups, they do so as an employee of the District and have responsibility for monitoring content and addressing inappropriate behavior on these networks.
- Be transparent. Your honesty—or dishonesty—will be quickly noticed in the social media environment. If you are posting about your work, use your real name and identify your employment relationship with the District. Be clear about your role; if you have a vested interest in something you are discussing, be the first to point it out. If you publish to a site outside the District's network, please use a disclaimer to state in clear terms that the views expressed are the employee's alone and that they do not necessarily reflect the views of the Bozeman School District.
- Protect confidential information. Students, parents, and colleagues should not be cited or obviously referenced on personal social networking sites without their approval.
- It is acceptable to discuss general details about projects, lessons, or events and to use nonidentifying pseudonyms for an individual (e.g., Teacher A) so long as the information provided does not make it

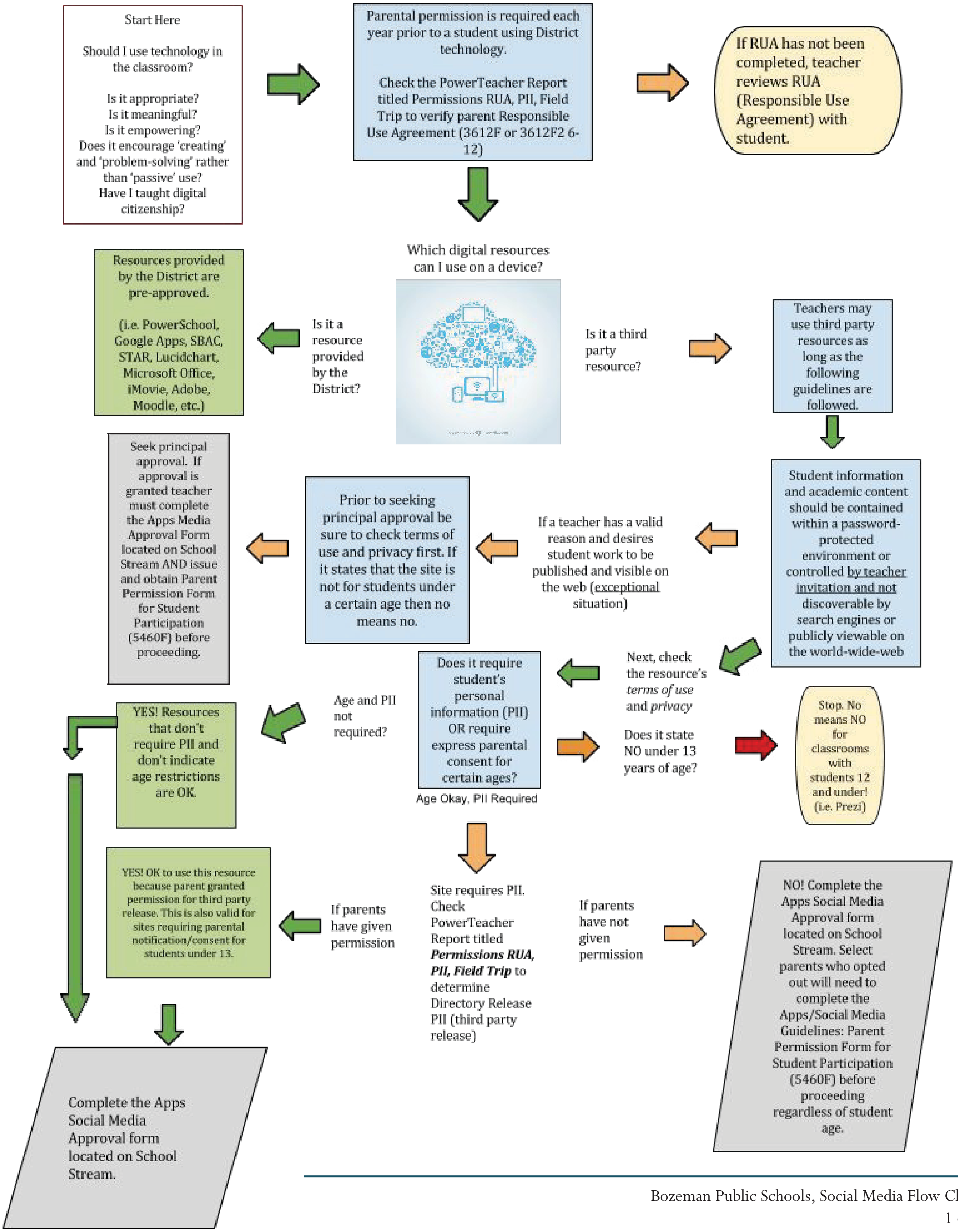
easy for someone to identify the individual or violate any privacy laws. Public social networking sites are not the place to conduct school business with students or parents.

- Respect your audience and your coworkers. Always express ideas and opinions in a respectful manner, including other schools or competitors. Remember that our community reflects a diverse set of customs, values and points of view. Be sensitive about linking to content. Redirecting to another site may imply an endorsement of its content.
- Perception can be reality. Just by identifying yourself as a District employee, you are creating perceptions about your expertise and about the District by community members, parents, students, and the general public; and you are creating perceptions about yourself with your colleagues and managers. If you chose to join or engage with District students and families in a social media context, do so in a professional manner, ever mindful that in the minds of students, families, colleagues and the public, you are a District employee. Be sure that all content associated with you is consistent with your work and with the District's beliefs and professional standards.
- Are you adding value? There are millions of words out there. The best way to get yours read is to write things that people will value. Communication associated with our District should help fellow educators, parents, students, and co-workers. It should be thought-provoking and build a sense of community. If it helps people improve knowledge or skills, do their jobs, solve problems, or understand education better—then it's adding value.
- Keep your cool. One of the aims of social media is to create dialogue, and people will not always agree on an issue. When confronted with a difference of opinion, stay cool. If you make an error, be up front about your mistake and correct it quickly. Express your points in a clear, logical way.
- Be careful with personal information. Make full use of privacy settings. Know how to disable anonymous postings and use moderating tools on your social media site(s). Astute criminals can piece together information you provide on different sites and then use it to impersonate you or someone you know, or even re-set your passwords.
- Be a positive role model, whether on or off duty. Both case law and public expectations hold educational employees to a higher standard of conduct than the general public.
- What in other mediums of expression could remain private opinions, when expressed by staff on a social networking website, have the potential to be disseminated far beyond the speaker's desire or intention, and could undermine the public perception of fitness of the individual to educate students, and thus undermine teaching effectiveness. In this way, the effect of the expression and publication of such opinions could potentially lead to disciplinary action being taken against the staff member, up to and including termination or non-renewal of the contract of employment.
- Don't forget your day job. You should make sure that your online activities do not interfere with your job. Remember that District technologies are provided for educational use. Use of District equipment and or social media during District time should be for educational purposes.

(Adapted with permission from Minnetonka Public Schools, Minnetonka, MN.)

Bozeman School District 5460, PERSONNEL - Electronic Resources and Social Networking
7 of 7

Using Online Learning Apps



Start Here

Should I use technology in the classroom?

Is it appropriate?
Is it meaningful?
Is it empowering?
Does it encourage 'creating' and 'problem-solving' rather than 'passive' use?
Have I taught digital citizenship?

Parental permission is required each year prior to a student using District technology.

Check the PowerTeacher Report titled Permissions RUA, PII, Field Trip to verify parent Responsible Use Agreement (3612F or 3612F2 6-12)

If RUA has not been completed, teacher reviews RUA (Responsible Use Agreement) with student.

Which digital resources can I use on a device?

Is it a resource provided by the District?

Resources provided by the District are pre-approved.

(i.e. PowerSchool, Google Apps, SBAC, STAR, Lucidchart, Microsoft Office, iMovie, Adobe, Moodle, etc.)

Is it a third party resource?

Teachers may use third party resources as long as the following guidelines are followed.

Student information and academic content should be contained within a password-protected environment or controlled by teacher invitation and not discoverable by search engines or publicly viewable on the world-wide-web

If a teacher has a valid reason and desires student work to be published and visible on the web (exceptional situation)

Prior to seeking principal approval be sure to check terms of use and privacy first. If it states that the site is not for students under a certain age then no means no.

Seek principal approval. If approval is granted teacher must complete the Apps Media Approval Form located on School Stream AND issue and obtain Parent Permission Form for Student Participation (5460F) before proceeding.

Next, check the resource's *terms of use* and *privacy*

Does it require student's personal information (PII) OR require express parental consent for certain ages?

Age Okay, PII Required

Age and PII not required?

YES! Resources that don't require PII and don't indicate age restrictions are OK.

Does it state NO under 13 years of age?

Stop. No means NO for classrooms with students 12 and under! (i.e. Prezi)

Site requires PII. Check PowerTeacher Report titled ***Permissions RUA, PII, Field Trip*** to determine Directory Release PII (third party release)

If parents have given permission

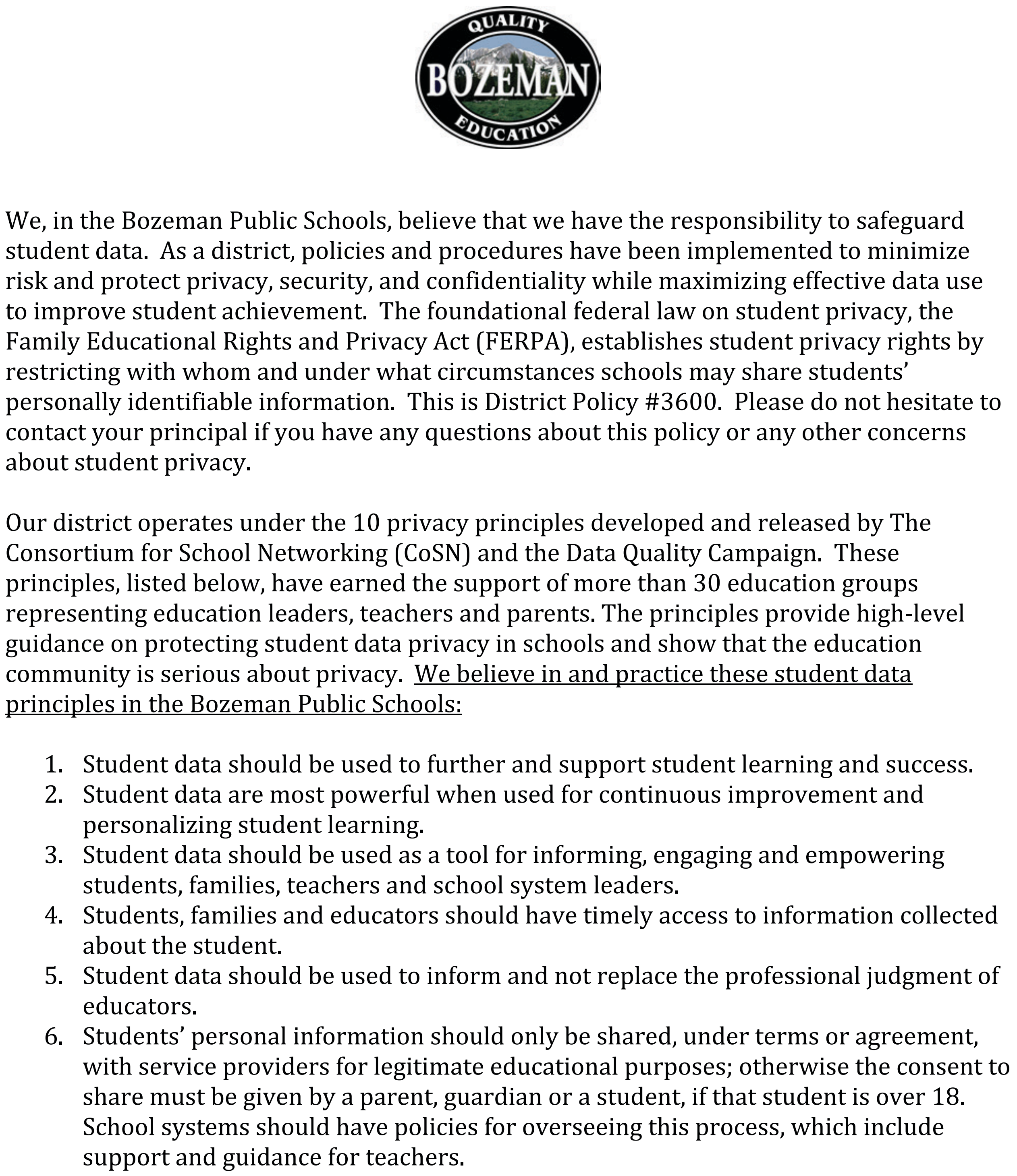
YES! OK to use this resource because parent granted permission for third party release. This is also valid for sites requiring parental notification/consent for students under 13.

If parents have not given permission

NO! Complete the Apps Social Media Approval form located on School Stream. Select parents who opted out will need to complete the Apps/Social Media Guidelines: Parent Permission Form for Student Participation (5460F) before proceeding regardless of student age.

Complete the Apps Social Media Approval form located on School Stream.

Bozeman Public Schools, Social Media Flow Chart
1 of 1



We, in the Bozeman Public Schools, believe that we have the responsibility to safeguard student data. As a district, policies and procedures have been implemented to minimize risk and protect privacy, security, and confidentiality while maximizing effective data use to improve student achievement. The foundational federal law on student privacy, the Family Educational Rights and Privacy Act (FERPA), establishes student privacy rights by restricting with whom and under what circumstances schools may share students' personally identifiable information. This is District Policy #3600. Please do not hesitate to contact your principal if you have any questions about this policy or any other concerns about student privacy.

Our district operates under the 10 privacy principles developed and released by The Consortium for School Networking (CoSN) and the Data Quality Campaign. These principles, listed below, have earned the support of more than 30 education groups representing education leaders, teachers and parents. The principles provide high-level guidance on protecting student data privacy in schools and show that the education community is serious about privacy. We believe in and practice these student data principles in the Bozeman Public Schools:

1. Student data should be used to further and support student learning and success.
2. Student data are most powerful when used for continuous improvement and personalizing student learning.
3. Student data should be used as a tool for informing, engaging and empowering students, families, teachers and school system leaders.
4. Students, families and educators should have timely access to information collected about the student.
5. Student data should be used to inform and not replace the professional judgment of educators.
6. Students' personal information should only be shared, under terms or agreement, with service providers for legitimate educational purposes; otherwise the consent to share must be given by a parent, guardian or a student, if that student is over 18. School systems should have policies for overseeing this process, which include support and guidance for teachers.

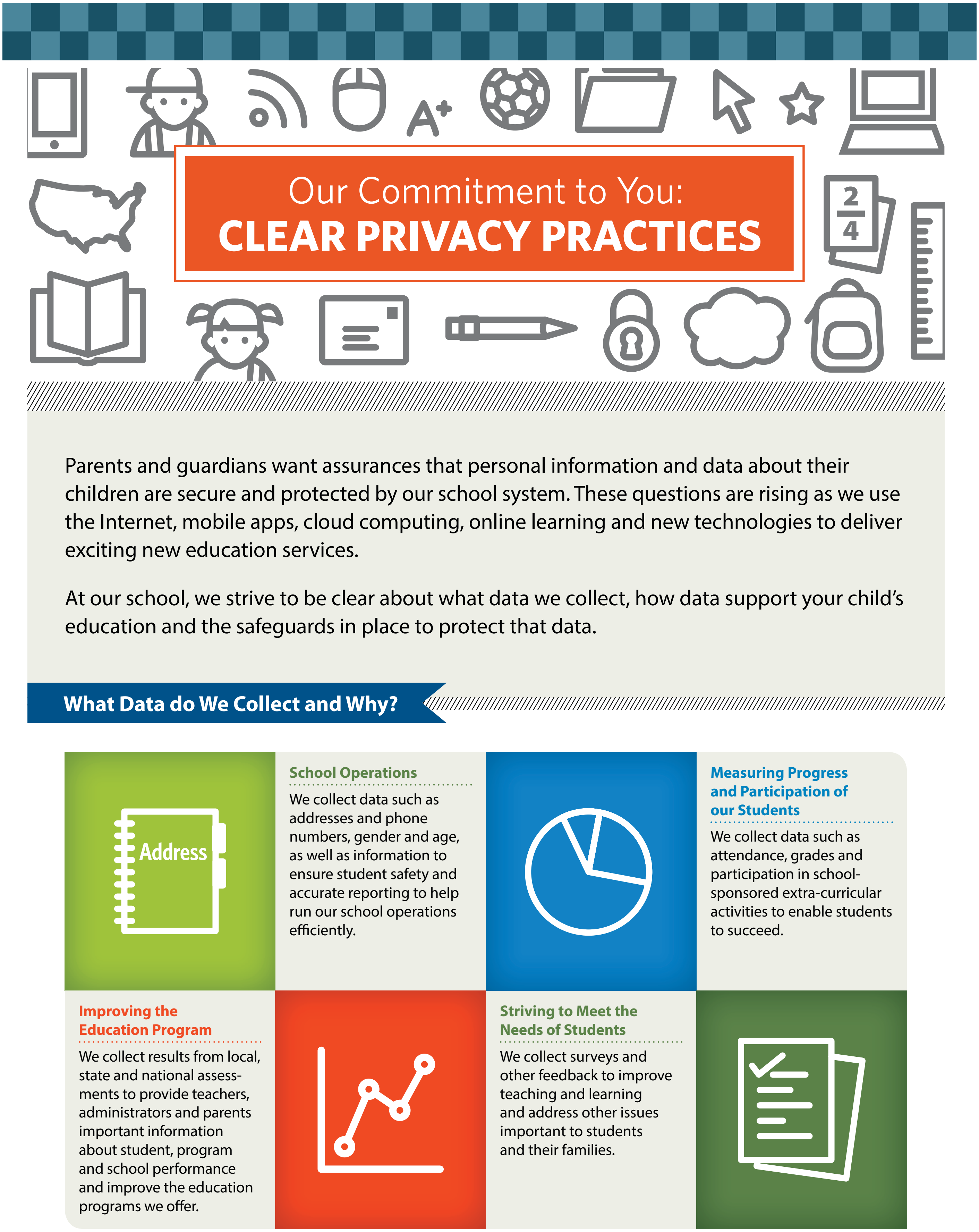
Bozeman Public Schools, Student Data Principles. Adapted with permission from CoSN.
1 of 4

7. Educational institutions, and their contracted service providers with access to student data, including researchers, should have clear, publicly available rules and guidelines for how they collect, use, safeguard and destroy those data.
8. Educators and their contracted service providers should only have access to the minimum student data required to support student success.
9. Everyone who has access to students' personal information should be trained and know how to effectively and ethically use, protect and secure it.
10. Any educational institution with the authority to collect and maintain student personal information should:
    - have a system of governance that designates rules, procedures and the individual or group responsible for decision-making regarding data collection, use, access, sharing and security, and use of online educational programs;
    - have a policy for notification of any misuse or breach of information and available remedies;
    - maintain a security process that follows widely accepted industry best practices; and
    - provide a designated place or contact where students and families can go to learn of their rights and have their questions about student data collection, use and security answered.

We, in the Bozeman Public Schools, share your concerns around privacy. In our district, we strive to be clear about why we collect data, how it is important to your child's education, as well as how we and our service providers protect that data. Please do not hesitate to contact your child's principal if you have any questions or concerns about this important topic.

Sincerely,

Rob Watson, Ed.D.
Superintendent



Our Commitment to You:
CLEAR PRIVACY PRACTICES

Parents and guardians want assurances that personal information and data about their children are secure and protected by our school system. These questions are rising as we use the Internet, mobile apps, cloud computing, online learning and new technologies to deliver exciting new education services.

At our school, we strive to be clear about what data we collect, how data support your child's education and the safeguards in place to protect that data.

What Data do We Collect and Why?

School Operations

We collect data such as addresses and phone numbers, gender and age, as well as information to ensure student safety and accurate reporting to help run our school operations efficiently.

Measuring Progress and Participation of our Students

We collect data such as attendance, grades and participation in school-sponsored extra-curricular activities to enable students to succeed.

Improving the Education Program

We collect results from local, state and national assessments to provide teachers, administrators and parents important information about student, program and school performance and improve the education programs we offer.

Striving to Meet the Needs of Students

We collect surveys and other feedback to improve teaching and learning and address other issues important to students and their families.

Bozeman Public Schools, Student Data Principles. Adapted with permission from CoSN.
3 of 4

How Do Education Data Support Student Success and School Improvement?

data=success!

TEACHERS need data to understand when students are thriving and when they need more support in learning specific concepts.

PARENTS and guardians need access to their child's educational data to help them succeed.

STUDENTS need feedback on their progress so they can make good decisions about program choices and prepare for success.

SCHOOL OFFICIALS and community members need to understand school performance and know if scarce education resources are being allocated fairly and effectively.

How is Education Data Protected?

We follow federal and state education privacy laws and adhere to privacy and security policies.

When we use an online service provider to process or store data, they also must adhere to certain federal and state and privacy laws. We also expect them to use current security protocols and technology.

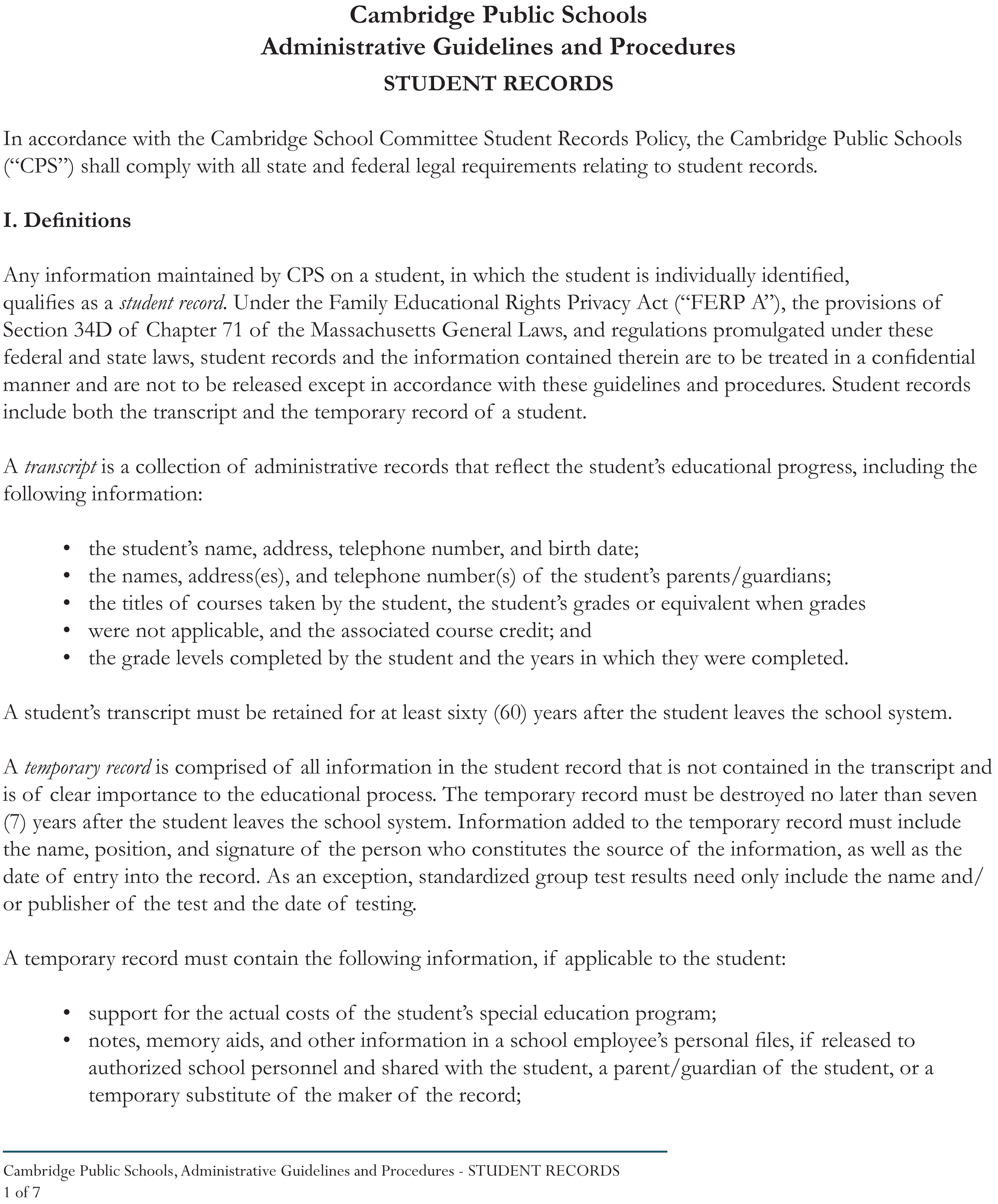
- For example, the Family Education Rights & Privacy Act (FERPA) gives parents rights related to their children's education records and personally identifiable information. Additional information is available in our annual notice to parents of their rights under FERPA and from the U.S. Department of Education at http://familypolicy.ed.gov/.
- Additionally, the federal Children's Online Privacy Protection Act (COPPA) prevents child-directed websites and apps from collecting certain personal information from anyone under 13 years of age without parental permission. Our school system may consent on behalf of parents in the education context when student information is collected for the school's exclusive use and benefit and for no other commercial purpose.
- Under FERPA, our vendors cannot use the education records we provide in any way that is not authorized by the school district. They cannot sell this data or allow others to access it except as we permit in accordance with federal and state education privacy laws.

Our Commitment

We are working to improve your children's education by ensuring it meets their unique needs. It would be very difficult to accomplish this goal without the ability to capture important information about your child's progress. Protecting personal information in secure and responsible ways is at the heart of our efforts to provide a richer and more dynamic learning experience for all students.

LEARN MORE about the rights of parents and guardians at **dataqualitycampaign.org/pta** or **PTA.org/Parents** or **commonsensemedia.org**

Bozeman Public Schools, Student Data Principles. Adapted with permission from CoSN.
4 of 4



Cambridge Public Schools
Administrative Guidelines and Procedures
STUDENT RECORDS

In accordance with the Cambridge School Committee Student Records Policy, the Cambridge Public Schools ("CPS") shall comply with all state and federal legal requirements relating to student records.

I. Definitions

Any information maintained by CPS on a student, in which the student is individually identified, qualifies as a *student record*. Under the Family Educational Rights Privacy Act ("FERP A"), the provisions of Section 34D of Chapter 71 of the Massachusetts General Laws, and regulations promulgated under these federal and state laws, student records and the information contained therein are to be treated in a confidential manner and are not to be released except in accordance with these guidelines and procedures. Student records include both the transcript and the temporary record of a student.

A *transcript* is a collection of administrative records that reflect the student's educational progress, including the following information:

- the student's name, address, telephone number, and birth date;
- the names, address(es), and telephone number(s) of the student's parents/guardians;
- the titles of courses taken by the student, the student's grades or equivalent when grades
- were not applicable, and the associated course credit; and
- the grade levels completed by the student and the years in which they were completed.

A student's transcript must be retained for at least sixty (60) years after the student leaves the school system.

A *temporary record* is comprised of all information in the student record that is not contained in the transcript and is of clear importance to the educational process. The temporary record must be destroyed no later than seven (7) years after the student leaves the school system. Information added to the temporary record must include the name, position, and signature of the person who constitutes the source of the information, as well as the date of entry into the record. As an exception, standardized group test results need only include the name and/or publisher of the test and the date of testing.

A temporary record must contain the following information, if applicable to the student:

- support for the actual costs of the student's special education program;
- notes, memory aids, and other information in a school employee's personal files, if released to authorized school personnel and shared with the student, a parent/guardian of the student, or a temporary substitute of the maker of the record;

- efforts by the principal/head of upper school regarding instructional practices and support responsive to student needs, the results of those efforts, and any consultation with the Assistant Superintendent for Student Services regarding accommodations and interventions for the student;
- documentation from the Assistant Superintendent for Student Services pertaining to the student's placement in a program that has not been approved by CPS, in accordance with the requirements of 603 C.M.R. § 28.06(e);
- specific, informed, written consent for a third party to access the student record;
- a copy of written expression by the student, if eighteen (18) years of age or older, limiting his/her parents' I guardians' rights with regard to the student record; and
- documentation indicating that a non-custodial parent's access to the student record is limited or restricted, ifit is so limited or restricted pursuant to 603 C.M.R. § 23.07(5)(a).

Please note that any recordings, film, photographs, audiotapes or videotapes of a student's image, likeness, spoken words, student work or learning experiences, performance and movement, in any form, that are created or are maintained by the school and/or school district are considered part of a student record and are subject to the federal and state laws and regulations governing student record information.

II. Access to Student Record Information

A student record may be accessed by the student's parents/guardians and/or by the student himself/herself, if he/she is an eligible student. For the purposes of access to student record information, an eligible student is a student who is fourteen (14) years of age or older and/or who has entered the ninth grade. Parents/guardians and eligible students may also authorize third party access to the student record. Please note that special procedures apply for processing requests for student records made by non-custodial parents. See pages 3-4 of these guidelines.

A student's parents/guardians and an eligible student have the right to inspect all portions of the student record or to receive a copy of any part of the student record upon request. The student record must be made available not later than ten (I 0) days after the request is made, unless the requesting party consents to a delay. Alternatively, a student's parent/guardian or an eligible student may request to have any part of the student record interpreted by a qualified professional of the school, or may invite any other person of his/her choosing to inspect and/or interpret the student record. If a student's parent/guardian and/or an eligible student is inspecting a student record, a school employee must remain present during the course of inspection to ensure the security of the record.

If a student is eighteen (18) years of age or older, the student's parents/guardians may access the student record until and unless the student expressly limits their access in writing.

School personnel working directly with a student may access information in the student record without the specific, informed, written consent of either the student or his/her parents/guardians. School personnel may only access student record information when such access is required in the performance of their official duties.

Except for a few limited exceptions, no other individuals or entities are allowed access to information in the student record unless the school has received specific, informed, written consent for the release of the specified information from the student's parent/guardian or the eligible student.

III. Requests by Non-Custodial Parents

Pursuant to 603 C.M.R. § 23.07(5), non-custodial parents (i.e. parents who do not have physical custody of their children) are eligible to obtain access to their children's student records unless the school or district has been given documentation evidencing:

- that the parent has been denied legal custody or has been ordered to supervised visitation, based on a threat to the safety of the student, specifically noted in the order pertaining to custody or supervised visitation;
- that the parent has been denied visitation;
- that the parent's access to the student has been restricted by a temporary or permanent protective order, unless the protective order or any subsequent order modifying the protective order specifically allows access to the information contained in the student record; or
- that there is an order of a probate and family court judge which prohibits the distribution of student records to the parent.

Non-custodial parents who fall into any of these categories may not have access to the student record and the school must place in the student record documentation indicating that the noncustodial parent's access to the student record is limited or restricted pursuant to 603 C.M.R. § 23.07(5)(a).

The non-custodial parent must submit a written request for the student record to the principal. In processing such a request the school must follow certain procedures:

1. Upon receipt of the request the school must immediately notify the custodial parent by certified and first class mail, in English and the primary language of the custodial parent, that it will provide the non-custodial parent with access after twenty-one (21) days, unless the custodial parent provides the principal/head of upper school with documentation that the non-custodial parent is not eligible to obtain access as set forth in 603 C.M.R. § 23.07(5)(a).
2. The school must delete all contact information (e.g. address, work and/or home telephone numbers, or e-mail addresses) of the custodial parent from the student record as provided to the non-custodial parent.
3. The student record as provided to the non-custodial parent must be marked with the phrase "**DOCUMENT CANNOT BE USED TO ENROLL STUDENT IN SCHOOL**."
4. Upon receipt of a court order that prohibits the distribution of information pursuant to Section 34H of Chapter 71 of the Massachusetts General Laws, the school shall notify the non-custodial parent that it shall cease to provide the non-custodial parent with access to the student record.

IV. Releasing Student Record Information

When a school receives a request for student record information to be released to an individual who is neither the student's parent/ guardian nor the student himself/herself, whether the request is written or oral, certain guidelines and procedures must be followed.

Requests by Third Parties

A request for student record information made by a third party must be accompanied by the specific, informed, written consent of the student's parent/guardian and/or the eligible student. A sample release form is attached to these guidelines and procedures for reference.

Requests by the Department of Children and Families

A request for student record information made by the Department of Children and Families ("DCF") may be concomitant with any of three sources _of authorization:

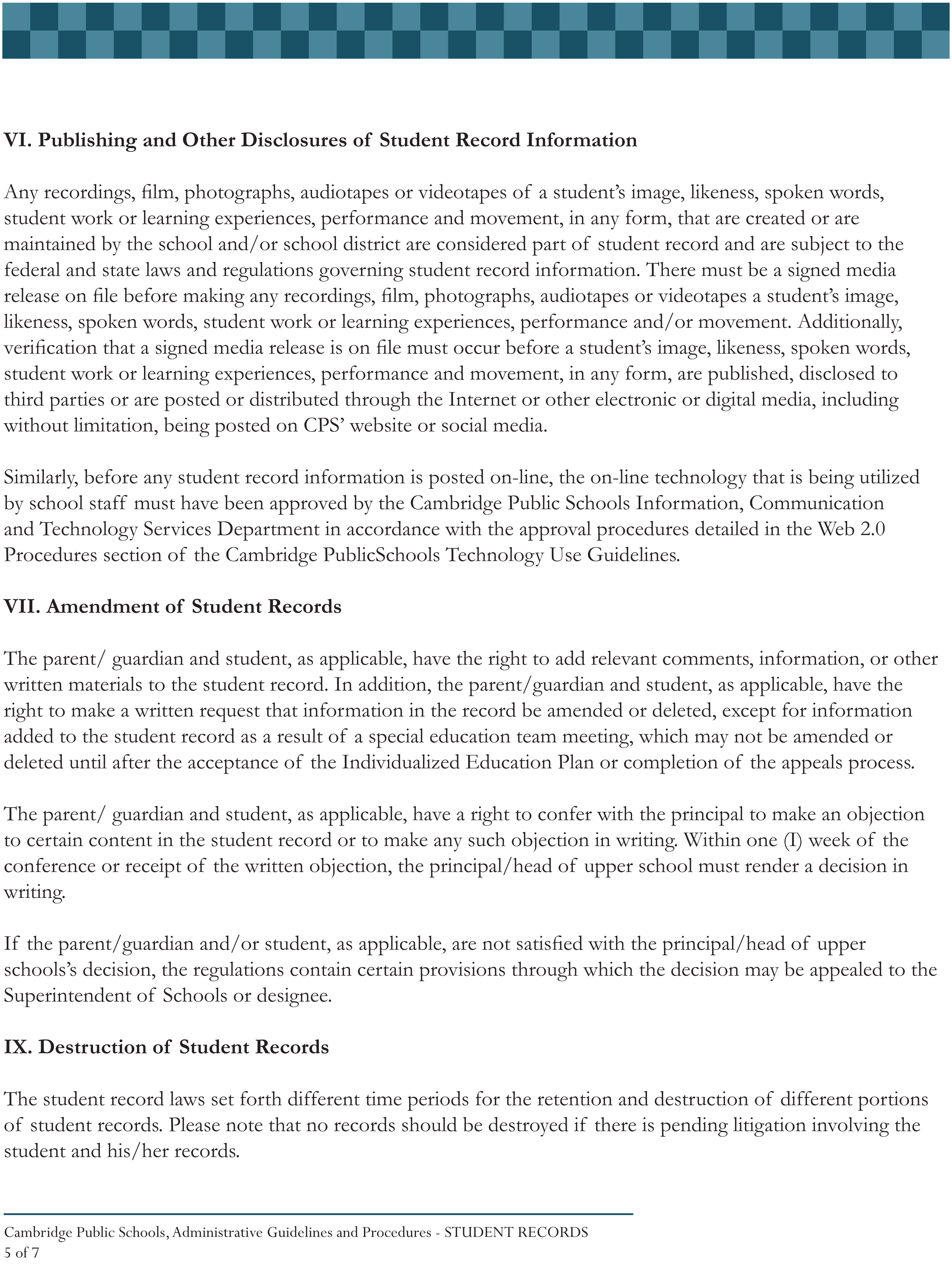
1. The request may be accompanied by the specific, informed, written consent of the student's parent/ guardian and/or the eligible student.
2. The request may be accompanied by a copy of a valid court order for the requested student record information. Although no consent is required to accompany the request, the student's parents/ guardians and/or the eligible student must be informed of the request before any student record information is released.
3. The request may be made in connection with DCF's investigation of a report of child abuse. In such cases, the request should be honored without a court order and without consent of the student's parent/guardian and/or the eligible student. The school, however, should document the name of the investigator making the request, photocopy the identification of the investigator, and confirm with the investigator's supervisor that such an investigation is being undertaken.

Subpoenas/Courts Orders

When a school receives a subpoena or court order for the production of student record information, a copy of that subpoena or court order should be forwarded promptly to the Office of Legal Counsel for processing of the required issuance of notices to parents/guardians regarding the subpoena and/or court order and required production of documents responsive to the subpoena and/or court order.

V. Providing Student Record Information to Other School Districts

When a student transfers to a new school district, the student, his/her parents guardians, or the school district from which he/she is transferring must provide the new school district with a complete copy of his/her student record, including any incidents involving suspension, expulsion, or any disciplinable offense.



VI. Publishing and Other Disclosures of Student Record Information

Any recordings, film, photographs, audiotapes or videotapes of a student's image, likeness, spoken words, student work or learning experiences, performance and movement, in any form, that are created or are maintained by the school and/or school district are considered part of student record and are subject to the federal and state laws and regulations governing student record information. There must be a signed media release on file before making any recordings, film, photographs, audiotapes or videotapes a student's image, likeness, spoken words, student work or learning experiences, performance and/or movement. Additionally, verification that a signed media release is on file must occur before a student's image, likeness, spoken words, student work or learning experiences, performance and movement, in any form, are published, disclosed to third parties or are posted or distributed through the Internet or other electronic or digital media, including without limitation, being posted on CPS' website or social media.

Similarly, before any student record information is posted on-line, the on-line technology that is being utilized by school staff must have been approved by the Cambridge Public Schools Information, Communication and Technology Services Department in accordance with the approval procedures detailed in the Web 2.0 Procedures section of the Cambridge PublicSchools Technology Use Guidelines.

VII. Amendment of Student Records

The parent/ guardian and student, as applicable, have the right to add relevant comments, information, or other written materials to the student record. In addition, the parent/guardian and student, as applicable, have the right to make a written request that information in the record be amended or deleted, except for information added to the student record as a result of a special education team meeting, which may not be amended or deleted until after the acceptance of the Individualized Education Plan or completion of the appeals process.

The parent/ guardian and student, as applicable, have a right to confer with the principal to make an objection to certain content in the student record or to make any such objection in writing. Within one (I) week of the conference or receipt of the written objection, the principal/head of upper school must render a decision in writing.

If the parent/guardian and/or student, as applicable, are not satisfied with the principal/head of upper schools's decision, the regulations contain certain provisions through which the decision may be appealed to the Superintendent of Schools or designee.

IX. Destruction of Student Records

The student record laws set forth different time periods for the retention and destruction of different portions of student records. Please note that no records should be destroyed if there is pending litigation involving the student and his/her records.

Destruction of Transcripts

A student transcript must be maintained for sixty (60) years following the student's graduation, transfer, or withdrawal from the school district. Only after the expiration of this sixty (60) year period should the student transcript be destroyed.

Periodic Review of Temporary Records

The principal/head of upper school or designee shall periodically review the temporary records of all currently enrolled students and identify for destruction any misleading, outdated, or irrelevant information. Prior to destroying any such information, the student and his/her parents/guardians must be given written notification of the intent to do so and be given the opportunity to receive a copy of the information prior to its destruction. Additionally, a copy of the written notice issued to the student and his/her parents/ guardians regarding the intent to destroy such information must be placed in the student's temporary record.

Destruction of Temporary Records

A student's temporary record shall be destroyed no later than seven (7) years after the student graduates, transfers, or withdraws from the school district. At the time of the student's graduation, transfer, or withdrawal from the school district, the student and his/her parents/guardians must be given written notification of the approximate date of destruction of the temporary record and their right to receive the information contained therein either in whole or in part. Such notice shall be in addition to the annual information letter issued by the school regarding standardized testing programs, research studies, and student record information.

X. Consequences for Failing to Comply with Student Record Regulations

CPS employees must observe all federal and state student record regulations, including those provisions regarding the confidentiality of student records and the information contained therein. CPS employees who release student record information in violation of federal law, state law, and/or these guidelines and procedures will be subject to disciplinary action, up to and including termination.

Additionally, pursuant to Section 34B of Chapter 71 of the Massachusetts General Laws, if a school official refuses or neglects to furnish a transcript by thirty (30) days after a request for the transcript was made, the student or former student requesting the transcript, or his/her parent/guardian or next friend if the student is a minor, may petition to the superior court of the county for enforcement.

Eligible students and parents/guardians can seek enforcement of student records statutes and regulations in court pursuant to 603 C.M.R. § 23.09.

XI. Annual Notification

At least once a year, each school should distribute a “policy statement” to all students and their parents/ guardians, provided in the student’s home language, either as part of its student handbook or as a separate document, informing students and their parents/ guardians of:

- standardized tests and research studies to be conducted during the year and other routine information to be collected or solicited from the student during the year;
- the right of students and their parents/guardians to have access to student records, to add relevant material, and to request deletion of objectionable material;
- the right of students and their parents/guardians to consent to disclosures of personally identifiable information contained in the student’s education records, except to the extent that FERPA and Section 99.31 of Title 34 of the Code of Federal Regulations authorize disclosure without consent;
- the right of students and their parents/guardians to file with the United States Department of Education a complaint concerning alleged failures by the school or CPS to comply with the requirements ofFERPA and Section 99;
- the procedure for exercising the right to inspect and review education records;
- the procedure for requesting amendment of records;
- a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest;
- notification that copies of the state regulations pertaining to student records are available to them at the school;
- notification that a student’s name, class, participation in officially recognized activities,
- sports, degrees, honors and awards, and post-high school plans may be released except for reasons of safety or health without their consent unless the student or his/her parent/ guardian informs CPS by October I each year that such information should not be released without their prior consent.

XII. Questions on Student Records

All inquiries concerning compliance with student records regulations or these guidelines and procedures should be addressed to the Office of Legal Counsel.

Policy references: *JRA, KEBA*
Legal references: *Mass. Gen. Laws, ch. 71, §§ 34 A-B, D-E, H, L; 603 C.MR. §§ 23.00, 28.00;*
20 US.C. § 1232g; 34 C.FR. § 99
Last updated: *August 18, 2014*