Case Studies

This document 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://sdpc.a4l.org/view_alliance.php?state=MA). 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.[1] 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).

[1] See https://sdpc.a4l.org/view_alliance.php?state=MA

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 https://studentprivacy.ed.gov/resources/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.

- 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.

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.

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 of the *Forum Guide to Education Data Privacy* 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?

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

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.

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 of the *Forum Guide to Education Data Privacy* 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 One of the *Forum Guide to Education Data Privacy*.

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.

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?

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.

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
    a. additional training requirements,
    b. counseling sessions, and/or
    c. 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 of the *Forum Guide to Education Data Privacy* for an overview of directory information policies under FERPA.