Privacy Handbook for Student Information Online: A Toolkit for Schools and Parents
**TABLE OF CONTENTS**

**I. Overview**  
The Data Analytics Pipeline (Thomas B. Norton)

**II. Tools for School Boards**  
Template: Board of Education Information Technology Governance Policy  
(Victoria Geronimo, Thomas B. Norton, N. Cameron Russell, Joel R. Reidenberg)

**III. Tools for School Administrators**  
Professional Development Materials – The Principal’s Guide to Understanding FERPA  
(Katherine Rosenberg)

FERPA Back to School Checklist and Materials for Administrators (Austen Ishii)

Selecting a Hosting Service Provider (Lauren Irby)

Selecting a Data Analytics Service Provider (Lauren Irby)


Data Breach Response Plan (Elizabeth Walker)

**IV. Tools for Teachers**  
Technology Security Checklist for Teachers (Elizabeth Walker)

Professional Development Materials- The Teacher’s Guide to Understanding FERPA  
(Katherine Rosenberg)

Professional Development Materials- FERPA FAQs (Katherine Rosenberg)

FERPA Do’s and Don’ts Guide for Teachers (Victoria Geronimo)

**V. Tools for Parents**  
FERPA Rights Infographic for Parents and Adult Students (Victoria Geronimo)
The Data Analytics Pipeline:
An Introduction to Educational Data Analytics and Related Concerns
Introduction

Schools increasingly employ technology to improve education and school administration. One study suggests that 95% of public school districts rely on web-based technologies for school functions—many of which are data analytics technologies.\(^1\) The primary functions of data analytics technologies are to aggregate and analyze student data.

Data analytics is a valuable tool for improving education: it can help determine when students are ready to learn new topics, when students are at risk, what grades a student might receive without teacher intervention, and whether a student needs academic help, among other benefits.\(^1\) While many products aid students in mastering certain subjects, some products additionally assist in other areas such as test preparation or state standard alignment.\(^1\)

Yet it is often unclear how data analytics products work. Common data analytics service providers often describe their products using broad, general language. For example, one vendor describes its product as “an innovative new solution that measures student engagement with digital course materials in order to provide administrators and faculty with actionable insights to help drive retention and outcomes.”\(^1\) Another vendor’s product is said to “accelerate[ ] achievement by enabling educators to connect the right learning resources to the right student at the right time.”\(^1\)

What do these statements mean? How do data analytics products achieve these results? What are some concerns surrounding the use of these products? To address these questions, let’s first explore the data analytics “pipeline”—that is, how data analytics products transform raw student data into meaningful results that improve education.

How Does Data Analytics Work?

Data analytics is one of the many technologies that schools and school districts use. Many of the data analytics products that schools use are online. This means that students study and complete assessments on computers that have some online learning system or software installed.\(^1\) When schools or school districts implement these systems, students use the systems to complete school-related assessments (alternatively, some products are available for individual, home use). When they use these systems, students engage in educational activity—such as doing homework or taking quizzes—online. The learning systems eventually provide the student with feedback in the form of individualized content, materials, and assessments. How do the systems do this?

Before using the system, students usually must obtain login credentials. When schools or districts employ a service, the school, district, or service provider usually creates and provides these credentials. Once a student has credentials, he or she may use the system.

Many of these systems collect detailed, personal data from students. For example, when students do school work on the systems, the systems can track how long it takes a student to complete a particular assignment,
how well he or she did on it, and even the content of the student’s responses. In addition to data about assignments, collected data may include passive data, such as the time a student logs in to the online learning system, the length of time he or she spends using the system, the computer’s IP address, and the web browsers the student uses. A student’s school may also input data about students from its internal information systems; schools usually maintain and input this data in electronic list format. All of this data is used to provide feedback on students and even to predict students’ future performance.

The systems use computerized mathematical processes called algorithms to store, sort, and present the collected data. Some products offer feedback in the form of visual dashboards, which allow students, parents, teachers, and administrators to access, view, and manipulate the data using system-specific analytic tools or programs like Excel.

Based on students’ current performance and predictions about their future performance, the online learning systems deliver to students, teachers, and schools learning materials that are appropriate for students’ current and predicted performance levels. Feedback provided by the online learning systems also allows teachers, administrators, and parents to view areas where students need help and enables those individuals to intervene in a timely manner to make sure students stay on track.

**Why Does Data Analytics Matter?**

Schools use data analytics to improve education and to gauge student, teacher, and school performance. For example, a student or parent might view the student’s personal dashboard to assess his or her progress, grades, or areas in which the student needs to improve; a teacher might view data about how students performed on an assignment to gauge their understanding of a particular topic; an administrator might look at an entire grade’s progress toward mastering his or her state’s educational standards, and might use the analytic tool to report the data to a state data system. In summary, data analysis technology provides real-time feedback that can aid teachers and administrators in allocating resources, assessing curriculum effectiveness, managing classrooms, and individualizing educational approaches. Consider the following anecdote:

> Dave is a fourth grade student. In class, he watches as his teacher sketches out the solution to a math problem on her interactive smartboard. Back home, he can log into the classroom app on his tablet to review the teacher’s notes as well as a short video showing her work through the problem. He then answers interactive questions and quizzes that are based on the lecture notes. His performance is automatically analyzed and he is steered to additional content, quizzes, and games that are tailored to his needs. He can communicate with his classmates and teacher about these problems through a social learning platform, participate in polls, and contribute to his classroom blog. Through the platform, he submits his homework assignment and the teacher grades it and provides immediate personal feedback. The teacher can track and monitor the progress of Dave and his classmates through a dashboard, identifying children who need additional assistance as well as those who are ready for more challenging exercises. This helps her decide whether to reiterate an issue for the entire class or devote additional time to Dave, so that, although he does not display it in
class, he can overcome his incoherence. Dave’s parents are apprised of his progress through an app, which provides access to his every assignment, grade, and test score—even the slides and videos used in class. Dave’s school obtains data helping it assess and adjust the fourth grade curriculum and evaluate the performance of students, classes, and teachers. The local school district judges the performance of Dave’s school and reports aggregate, anonymous data to the state department of education. Funding is directed to schools that are successful at improving children’s readiness for college and to districts that hold teachers accountable for student performance.¹

As this example demonstrates, data analytics (as well as other education technologies) carries the potential to improve education dramatically. But data analytics requires the collection of students’ sensitive, personal information. This raises concern: some believe that companies operating in the education technology sphere seek profit at the expense of students’ privacy and future reputation. Consider a different version of the above anecdote:

Dave is a fourth grade student. His interaction with his teacher has become entirely mediated by screens, including tablets, software, dashboards, and apps. Algorithms that crunch through his every keystroke and page-view constantly assess him. His school experience is focused on test preparation, evaluations, and exams. The software used by his school is made by a for-profit company, and vendors, which are advised by think tank experts, develop the curriculum and tests. The school has put Dave’s teacher on probation since she “couldn’t make her target numbers.” Her plea to reason, arguing that her students have special needs and should not be judged against national or state metrics, fails to impress her principal, who in turn is under increasing pressure from the school district and state to improve student performance, as judged by standardized test scores. The data collected from Dave and his classmates is stored by a cloud service provider, which centrally hosts sensitive information from hundreds of schools. Fifteen years later, as Dave seeks to enter the workforce, a prospective employer inquires about his suspension from Ms. Smith’s fourth grade class.¹

The good news is that student data privacy seems to be on the minds of data analytics service providers. For example, it is one company’s policy to educate customers about student privacy laws.¹ It is the same company’s policy to also ensure that customer data does not come through its support department when that department assists customers, lest it risk violating student privacy laws on customers’ behalf.¹ This policy results from a great concern about student data privacy expressed by school officials during the company’s product bidding, implementation, and support processes; the company recognizes that school officials are concerned with making sure that personally identifiable student data is encrypted and not transferred in any way.¹

What’s Next?

This handbook will provide resources for boards of education, school administrators, teachers, and parents. These resources, which take the form of ready-to-use “toolkits,” will assist members of those groups in understanding student privacy issues and in protecting student privacy.


1 Telephone Interview with Edmentum salesperson (Oct. 21, 2014).


1 See supra note 3.

1 Telephone Interview with Edmentum tech support (Oct. 27, 2014).


1 Id.

1 Telephone Interview with eScholar tech support (Oct. 27, 2014).

1 Id.

1 Id.
Template:
Board of Education
Information Technology
Governance Policy
## I. Mission Statement

The [DISTRICT NAME] Board of Education recognizes the use of technology in the educational process as an essential part of the schooling experience. Technology is to be viewed as a resource to enhance the learning process among other resources available to teachers and pupils. In addition, technology can be used to enhance the administration of the schools and the district. In order to provide direction and meaning to the use of technology as an instructional resource, the Board encourages and supports staff use of technology as a component of the learning process. Adoption and use of technology in District schools should be guided by the Board’s Technology Goals, as listed in Section II.

## II. Technology Goals

The Board adopts the following goals for the District’s technology use:

[GOALS¹]

## III. Technology Plan

The Superintendent or his designee² shall devise and implement a Technology Plan. The Plan should describe how the [EDUCATIONAL INSTITUTIONS] will achieve the technology goals described in Section II.

---

¹ See APPENDIX A – SAMPLE BOARD OF EDUCATION TECHNOLOGY GOALS for suggestions.
² This administrator, for example, would be a Director of Technology, Chief Technology Officer or other person responsible for technology-related matters for the district.
| **IV. REQUIRED EVALUATION AND APPROVAL OF SOFTWARE AND COMPUTER SERVICES** | The Superintendent or his designee shall evaluate all software and computer services involving any student information before such software or computer services are approved for District use. When evaluating software or a computer service, the Superintendent or his designee must at a minimum assure that the software or computer service:

a) meets the Technology Goals described in Section II;

b) adequately protects student privacy;

c) complies with applicable federal and state privacy laws, regulations, and community standards; and

d) assures adequate security.

The satisfaction of these minimum requirements must be evidenced in a signed, written agreement between the District and the vendor of any software or computer service to be used by the District.

No software or computer services involving student information may be used by the District or District personnel unless approved by the Superintendent or his designee in accordance with the approval procedure set forth in this policy.

The District shall maintain a current list of all approved software and computer services.

| **[OPTIONAL ALTERNATIVE, recommended if resources allow]** |
| **CHIEF PRIVACY OFFICER** |
| The Superintendent shall appoint, as his designee, a Chief Privacy Officer (“CPO”) to evaluate all software and computer services involving any student information before such software or computer services are approved for district use. |

| **V. APPROVAL AND ADOPTION PROCESS** | The Superintendent shall develop a procedure for approving the use and acquisition of new technology services. |
| VI. IMPLEMENTATION PLAN AND TRAINING | The Superintendent or his designee shall develop a plan for implementing new technologies at district schools so that use of such technologies complies with this Policy and shall promulgate administrative regulations, guidelines, and user agreements consistent with the District’s technology mission and goals, with law, and with this Policy.

The Superintendent or his designee shall assign trained personnel to maintain the District’s technology in a manner that will protect the district from liability and will protect confidential student and employee information retained in or accessible through District technology resources.

The Superintendent or his designee shall require that district staff be trained in the use of any new technologies, and shall provide training to staff and teachers as is applicable and necessary to achieve the District’s technology goals. |
| VII. AUDIT AND REVIEW | The [CHIEF SCHOOL ADMINISTRATOR] shall periodically audit and review the use of technology throughout the District. Such review should ensure that instructional resources and equipment that support and extend the curriculum are available to teachers and students. Such review shall further ensure that the District complies with the procedures mandated by this Policy and that the District complies with applicable law. |
APPENDIX A – SAMPLE BOARD OF EDUCATION TECHNOLOGY GOALS

The following are examples of Board of Education Technology Goals available for adoption by your district’s board of education. For example, your board of education may adopt technologies:

1. “To ensure that all activities, expenditures, actions, and efforts are designed and undertaken to enhance student performance.”

2. “To ensure continual improvement of quality while ensuring effective use of the District’s resources.”

3. “To maximize the likelihood of project success and minimize both the occasion for errors and the time required for implementation.”

4. “To ensure the availability of information to those who need it when they need it.”

5. “To provide direction and focus for technology activity.”

6. To provide “a resource to enhance the learning process among other resources available to teachers and pupils.”

7. To “enhance the administration of the schools and the district.”

8. To “improve student performance and achievement, increase staff productivity, and assure[ ] greater efficiency in the operations and communications of the school system.”

9. To “tap into ‘depositories of research,’ . . . retrieve resource information for in-depth research, [and to] complement the present ‘traditional’ media center sources.”

10. “[T]o stimulate and augment a more powerful and productive learning environment.”

---

4 Id.
5 Id.
6 Id.
7 Id.
9 Id.
10 Sublette County School District #9, Policy IHAJ – Network/Internet Usage Policy, Adopted: July 2011.
11 Id.
12 Id.
OVERVIEW

I. What is FERPA?
II. What rights does FERPA provide?
III. What information does FERPA protect?
IV. What are my specific duties, as principal, under FERPA?
V. How can I ensure my school is FERPA-compliant?

OBJECTIVES

By the end of these slides, you should:

1. Understand what FERPA is and what rights it grants.
2. Be able to distinguish what information may be disclosed with and without consent under FERPA.
3. Identify your responsibilities as administrator to ensure your school complies with FERPA.
4. Feel more comfortable disseminating information about FERPA to your staff.
WHAT IS FERPA?

THE BASICS

In this section...

- What is FERPA?
- Who is granted rights under FERPA?
- Who enforces FERPA?
- Is my school subject to FERPA?

WHAT IS “FERPA”?

FERPA =

FAMILY
EDUCATIONAL
RIGHTS &
PRIVACY
ACT

THE BASICS

What is FERPA?

- FERPA is a federal law that protects the confidentiality of student education records.
- Schools must adopt procedures to comply with FERPA.
- As principal, it is important to understand FERPA’s requirements and how they affect school administration.

FERPA is a federal law, provided in Title 20 of the United States Code (U.S.C.). There are also federal regulations regarding FERPA, provided in Title 34 of the Code of Federal Regulations (C.F.R.). Both the statutory text and regulations of FERPA are helpful to understand how to comply with its provisions!
THE BASICS  

Who is granted rights under FERPA?

- Parents.
- Rights transfer to students when they turn **18** years old OR attend a postsecondary institution ("eligible students"), but...
- Parents who claim children as dependents on their taxes retain their rights.

General Rules of Thumb
- Parents have FERPA rights unless their adult child is not claimed as their dependent.
- Students 18+ have FERPA rights.

THE BASICS  

Who enforces FERPA?

- FERPA is administered by the Family Policy Compliance Office (FPCO) in the Department of Education.
- If a parent or eligible student files a FERPA complaint against your school, the FPCO may investigate your school's procedures to determine what action should be taken.

In the event of a violation, the FPCO will inform your school of the steps it must take to comply with the law.

THE BASICS  

Is my school subject to FERPA?

- FERPA applies to all schools that receive federal funding for any program administered by the Dept. of Education.

If your school is a public school or receives federal funding for programs, FERPA applies!
WHAT RIGHTS DOES FERPA PROVIDE?

FERPA gives parents (and eligible students) the right to:

1. **Consent to the disclosure** of personally identifiable information from education records, *except as required by law*;
2. **Review and inspect** student education records; and
3. **Request correction** of these education records.

WHAT RIGHTS DOES FERPA PROVIDE?

FERPA REQUIREMENT: 

1. Right to **CONSENT to DISCLOSURE** of personally identifiable information (PII).

**YOUR SCHOOL MUST:**

- Obtain written permission before releasing PII from a student’s education record.*
- Send annual notice to parents/eligible students on what constitutes directory information.
- Ensure your school only employs third-party service providers that securely protect student data.

*Unless the recipient is the eligible student, or his or her parent!
WHAT RIGHTS DOES FERPA PROVIDE?

FERPA REQUIREMENT: 2. Right to INSPECT & REVIEW student’s education records maintained by the school.

YOUR SCHOOL MUST:
- Designate an officer responsible for responding to parent/eligible student requests.
- Respond to requests within 45 days of receipt.
- Allow access to records or provide copies of records (if access isn’t feasible).

WHAT RIGHTS DOES FERPA PROVIDE?

FERPA REQUIREMENT: 3. Right to REQUEST CORRECTION of records they believe are inaccurate/misleading.

YOUR SCHOOL MUST:
- Evaluate requests to amend records
- Amend records, if appropriate, or...
- Hold a formal hearing if school denies request (If request is denied after hearing)
- Allow parent/eligible student to add a statement within the record setting forth his or her view about the contested information.

WHAT INFORMATION DOES FERPA PROTECT?

In this section...
- Overview of FERPA-protected information
- What are “education records”?
- What is “directory information”?
- What rules govern disclosure of education records?
WHAT INFORMATION DOES FERPA PROTECT?

FERPA prevents disclosure of information from a student’s “education record,” but doesn’t prevent disclosure of “directory information.”

In the following slides, you’ll learn the difference between education records and directory information.

EDUCATION RECORDS are...

Records directly related to a student that are
• maintained by the school, or
• maintained by a third-party vendor, on behalf of the school.

FERPA prohibits release of education records without consent of parents or the eligible student.

Any vendor your school uses that collects and stores student information/data, purposefully or incidentally:
• Ex: data-hosting services, online learning programs

Check the Text! See the definition of “education records” in the text of FERPA.

EXAMPLES OF EDUCATION RECORD INFORMATION:

• Student grades
• Immunization & health records maintained by the school
• Disciplinary records
• Student progress reports
• Academic or physical testing results
• Grade point average
• Attendance records

Your school MUST keep information in a student’s education record confidential and secure.
**INFORMATION that ISN’T IN AN “EDUCATION RECORD”**

- Private records kept in the sole possession of the teacher (or substitute) for memory purposes.
- Law enforcement or campus security records created and maintained solely for law enforcement reasons.
- Employment records (unless employment is contingent upon enrollment and attendance)
- Alumni records
- Grades on peer-graded papers before they’re recorded

**“EDUCATION RECORDS”**

**KNOWLEDGE CHECK: Education Record? Yes or No**

- Log of student’s disciplinary history ✓ Yes
- Student’s health records created by school nurse ✓ Yes
- Teacher’s written notes for own use ✓ No
- Records kept by campus security re: vandalism incident ✓ No
- Teacher’s gradebook ✓ Yes
- Student transcript ✓ Yes

**WHAT INFORMATION IS PROTECTED UNDER FERPA?**

**CHECK YOUR KNOWLEDGE**

A teacher sees or hears a couple of students fighting in the hall, and his or her knowledge of the events only comes from this direct observation.

*Does FERPA govern disclosure of what he or she saw?*
WHAT INFORMATION IS PROTECTED UNDER FERPA?

**ANSWER**

No, FERPA does not prohibit a school official (here, the teacher) from disclosing information he or she witnessed. Direct observations aren't part of a student's education record.

- A school official may disclose what he or she overheard to appropriate authorities, including disclosing the information to local law enforcement, other school officials, and parents.
- If that information is included in the student's disciplinary record after the teacher reports it, then it becomes part of that student's education record.

---

PERSONALLY IDENTIFIABLE INFORMATION

Information that, alone or in combination, would generally allow a person in the school community to identify a student with reasonable certainty.

FERPA prohibits the release of "personally identifiable information" contained in a student's education record, unless it is directory information...

---

DIRECTORY INFORMATION is...

Personally identifiable information that is not generally considered harmful if disclosed.

- FERPA allows schools to disclose this information without consent, as long as they provide public notice to families that explains what types of information the school has designated as "directory information."

Check the Text!
See the FERPA text regarding what is "directory information."
COMMON EXAMPLES OF “DIRECTORY INFORMATION”

- student’s name
- address
- telephone number
- date of birth
- major field of study
- participation in officially recognized activities/sports
- weight & height of athletic team members
- dates of attendance
- degrees/awards received
- most recent previous educational institution attended by student
- e-mail address
- place of birth
- photograph
- grade level
- enrollment status

“DIRECTORY INFORMATION”

YOUR SCHOOL MUST:

☐ Send annual notice to parents/eligible students that
  ☐ explains they have a right to refuse to allow the school to designate any/all of these categories as their directory information, and
  ☐ gives a reasonable period of time for this refusal before any directory information is disclosed.

NOTE!
Notice may take many forms—a letter, section of a handbook, in summer mailings—as long as it gives families adequate time to respond before any directory information is disclosed!

Click here for the FPOO’s “Model Notice for Directory Information,” an example of the annual notice sent to families.

“DIRECTORY INFORMATION”

Designating directory information categories (and providing clear and adequate notice) allows your school to celebrate your students in playbills, rosters, or in your local newspaper without violating FERPA!
A Recap: What Information Does FERPA Protect?

**Education Records**
Information directly related to a student and that is maintained by the school, or a party acting on the school's behalf.

**Directory Information**
Information, designated through notice by the school, that would not generally be considered harmful if an invasion of privacy occurred.

**MAY NOT**
be disclosed without consent.

**MAY**
be disclosed without consent.

But, there are some special circumstances that allow disclosure of education records without consent...

Disclosures

Check the Text!
See the full FERPA text regarding when disclosure of education records is permitted.

Special Circumstances for Disclosure of Education Records

- School officials with legitimate educational interests;
- Other schools to which a student is transferring;
- Specified officials for audit/evaluation purposes;
- In connection with financial aid to a student;
- Accrediting organizations;
- To comply with judicial orders/subpoenas;
- Appropriate officials in health/safety emergencies
- State & local authorities pursuant to State law.

Check Out the Text!
In addition to the text of FERPA, see the federal regulations for more help determining when records may be disclosed.
WHAT ARE MY SPECIFIC DUTIES UNDER FERPA?

If your school doesn’t already have a school official responsible for FERPA-compliance,

- Select a staff member (preferably with a strong technology background or responsible for the technology program) \( \Rightarrow \) RECOMMENDED
- Or, retain the position and fulfill these obligations.
- Train staff members on their FERPA requirements.

HOW CAN I ENSURE MY SCHOOL IS FERPA-COMPLIANT?
HOW CAN I ENSURE MY SCHOOL IS FERPA-COMPLIANT?

- Send annual notification of:
  - FERPA rights and "directory information" categories
- Respond to parent/eligible student education record requests within 45 days.
- Maintain a record of every request for access to and disclosure from an educational record.
- Evaluate all other requests for student information to determine if a possible FERPA violation might occur.
- Consider all requests to correct/amend education records.
  - If school decides not to amend, hold a hearing.
  - If, after hearing, school decides not to amend, allow parent/eligible student to insert statement in the record setting forth own views.
- Ensure staff is properly trained on proper procedures for responding to access or disclosure requests.
- Evaluate third party vendors to determine if they can/do comply with FERPA requirements.

RESOURCES

- Annual notification requirements
- Sample response to record access request
- Sample response to record correction request
- Sample notification of formal hearing for a record correction
- Guidelines for evaluating requests for disclosure of student information

APPENDIX

HELPFUL MATERIALS AND LINKS
GLOSSARY

Directory Information: information designated by a school that is more basic and is not harmful if disclosed.

Education Records: records maintained by the school that are directly related to a student

Eligible Student: A student who is either 18 years of age or older, or is attending a post-secondary institution.

FERPA: Family Educational Rights & Privacy Act, federal law that governs confidentiality of student educational records.

FPCO: Family Policy Compliance Office, enforces FERPA.

Personally Identifiable Information: contains information that would make the student’s identity and any related information about him or her easily recognized.

HELPFUL RESOURCES

FERPA STATUTE AND REGULATIONS
Full Text of FERPA - Cornell Law Website
FERPA Federal Regulations - Cornell Law Website

OTHER MATERIALS
• FPCO Website for Parents
• FPCO Additional Slides for School Leaders – October 2012
• FPCO PDF for Parents – February 2011
• FPCO Guidance for Parents – October 2007
• National Center for Education Statistics - Resources for FERPA Access
• PTAC Disclosure Exceptions Rubric
• Additional FERPA Lesson Plan – Calhoun Intermediate School District
  * Accompanying FERPA/HIPAA Quiz – CISD

BIBLIOGRAPHY
This presentation was created using materials from the following institutions:
• The Family Policy Compliance Office (FPCO)
• Data for Student Success (Data4SS.org)
• Skyline High School, Ann Arbor, MI
• Cornell University Law School
• National Center for Education Statistics (NCES)
FERPA Back-to-School Checklist & Materials for Administrators


These materials may be reproduced, in whole or in part, for educational and non-commercial purposes provided that attribute is included.
FERPA BACK-TO-SCHOOL CHECKLIST:

Before sending out the Annual FERPA Notification Letter and Notice of Directory Information, it is important that administrators (1) take the time to consider and understand the information that they are distributing to parents and students; and (2) put in place the necessary polices and procedures to properly handle any questions or FERPA requests that may result from the distribution of the notices.

To help ensure that the school is complying with its statutory obligations, administrators should consider the following readiness checklist as they prepare to send out the FERPA notifications with the rest of their back-to-school materials:

Appointing a FERPA official (Records Custodian):

- Appointed ______________________ on ______ to act as FERPA Records Custodian.

<table>
<thead>
<tr>
<th>Name of Appointed Official</th>
<th>Date</th>
</tr>
</thead>
</table>

  The Records Custodian will have the following duties:

  - Monitoring any incoming FERPA requests from parents and students, and responding to them within 45 days.
  - Identifying which materials may be disclosed upon receipt of a request and which may not be disclosed.
  - Providing access to properly requested educational records.
  - Recording each FERPA request that is received and processed, and detailing what access, if any, was ultimately provided to student records.
  - Identifying what the school has listed as directory information, and the opt-out procedure for directory information.
  - Implementing a standardized procedure for amending student’s educational data.

Adopting the Necessary Policies and Procedures:

- Outlined and adopted a procedure for recording the receipt, processing, and response to FERPA requests on ______. That procedure is attached as: _____________________________.

<table>
<thead>
<tr>
<th>Date</th>
<th>Document Name</th>
</tr>
</thead>
</table>

- Outlined and adopted a procedure for providing access to student’s educational records on ______. That procedure is attached as: _____________________________.

<table>
<thead>
<tr>
<th>Date</th>
<th>Document Name</th>
</tr>
</thead>
</table>

- The school will: (Check all that apply)
  - Provide access to student’s records; or
  - Send copies of materials to parents and students at a cost of $_____/page.

  ____________________________ has considered how to provide access to such records without revealing data pertaining to any student other than that identified in the FERPA request.

- Outlined and adopted a procedure for amending student records on _______.

  That procedure is attached as _____________________________.

<table>
<thead>
<tr>
<th>Date</th>
<th>Document Name</th>
</tr>
</thead>
</table>

- Outlined and adopted a procedure for allowing parents and students to opt out of disclosure of directory information on ______. Attached as _____________________________.

<table>
<thead>
<tr>
<th>Date</th>
<th>Document Name</th>
</tr>
</thead>
</table>
Reviewing the Data Your School is Collecting:

<table>
<thead>
<tr>
<th>Service Providers, applications, databases, or other systems storing, processing or using student data:</th>
<th>Purpose / description of use:</th>
<th>Groups or individuals with access:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DOCUMENT 1:
Model Annual FERPA Notification Letter
Annual FERPA Notification for 20[ ]-20[ ] Academic Year

Dear [SCHOOL NAME] parents and students,

Each year, [SCHOOL NAME] provides information regarding the Family Educational Rights and Privacy Act (FERPA). This federal law is designed to provide some confidentiality for students’ educational records. FERPA also gives you, or your child (if they are 18 years of age or older), the ability to access your child’s educational records, and make certain decisions about those records. FERPA provides you or your child with four basic rights:

1. Disclosure

[SCHOOL NAME] must get written consent from parents, guardians, or students 18 years of age or older before disclosing a student’s personally identifiable information, with a few exceptions.

How it works:

• Generally the school must get written permission before sharing a student’s information with others. However, the school may share a student’s information with school officials who have legitimate educational interests, without obtaining written permission. School officials may include many different individuals such as school employees, volunteers, contractors, consultants, official committees, and others who might need to review a student’s educational records in order to fulfill professional responsibilities.

• [SCHOOL NAME] also discloses education records without consent to officials of another school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student’s enrollment or transfer, upon request from those school officials.

2. Inspection

Parents, guardians, or students 18 years of age or older may inspect and review the student’s educational records.

How it works:

• Parents, guardians, or eligible students must submit a written request to [APPROPRIATE SCHOOL OFFICIAL] that identifies the record(s) that they wish to inspect.

• Within 45 days of receiving the request, the school official will either make arrangements for access and notify the parent, guardian or eligible student of the time and place where the records may be inspected, or the school may provide copies of the records, or portions of the records, for a fee.
3. Amendment

Parents, guardians, or students 18 years of age or older may ask school officials to amend a student’s educational records that they believe are inaccurate, misleading, or which violate the student’s privacy rights under FERPA.

How it works:

• Parents, guardians, or eligible students must submit a written request to [APPROPRIATE SCHOOL OFFICIAL] clearly identifying the part(s) of the record that they want changed, and specifying why the record(s) should be changed.

• The school will decide whether or not to amend the record(s) as requested, and then notify the parent, guardian, or eligible student of the school’s decision. The school will also notify the parent, guardian, or eligible student of their right to a hearing regarding the request for amendment, and provide information on how to set up such a hearing.

4. Complaint

Parents, guardians, or students 18 years of age or older may file a complaint with the U.S. Department of Education concerning alleged failures by the [SCHOOL NAME] to comply with the requirements of FERPA.

How it works:

• Parents, guardians, or eligible students can contact the U.S. Department of Education office in charge of administering FERPA:

  Family Policy Compliance Office
  U.S. Department of Education
  400 Maryland Avenue, SW
  Washington, DC 20202

If you have questions about the information above, you can contact [APPROPRIATE SCHOOL OFFICIAL], at [CONTACT INFO].

The following websites also provide helpful information about FERPA:

• The U.S. Department of Education’s FERPA page: www2.ed.gov/ferpa
• The Future of Privacy Forum’s FERPA SHERPA project: www.ferpasherpa.org
DOCUMENT 2:
Model Annual Notice of Directory Information
[SCHOOL NAME]’s Notice of Directory Information for 20[ ]-20[ ] Academic Year

The Family Educational Rights and Privacy Act (FERPA), generally requires [SCHOOL NAME] to obtain your written consent prior to the disclosure of personally identifiable information from a student’s education records. However, [SCHOOL NAME] may disclose “directory information” without written consent, unless you have notified the school otherwise.

What is Directory Information?

Directory information is basic information related to a student that the school may included in certain school publications such as yearbooks, graduation programs, sports activity sheets, honor roll or other recognition lists, etc.

[SCHOOL NAME] currently designates the following information as directory information:

- Student’s 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 educational agency or institution attended
- Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems that cannot be used to access education records without a PIN, password, etc. (A student’s SSN, in whole or in part, cannot be used for this purpose.)

Who might receive Directory Information?

Releasing directory information is generally not considered harmful or an invasion of a student’s privacy. Some examples of outside organizations that might receive directory information include companies that manufacture class rings or publish yearbooks. In addition, two federal laws require schools receiving certain federal funds to provide military recruiters, upon request, with the following information – names, addresses and telephone listings – unless parents have informed the school that they do not want their student’s information disclosed without their prior written consent.
How can I opt-out of Directory Information disclosure?

Directory information is considered public information and will be released unless the student requests a “privacy hold.” If you do not want [SCHOOL NAME] to disclose directory information from your child's education records without your prior written consent, you must notify the District in writing by [DATE].

All other information is considered private, and will not be released outside the school without the written permission of the student, unless a specific exception under FERPA applies.

Questions concerning student rights under FERPA should be addressed to [APPROPRIATE SCHOOL OFFICIAL].
DOCUMENT 3: Sample Tracking Sheets
SAMPLE FERPA Request Tracking Table

<table>
<thead>
<tr>
<th>Date of FERPA Request:</th>
<th>Student Identified:</th>
<th>Records/Information Requested:</th>
<th>Requestor’s Contact Information (name, phone, address, etc):</th>
<th>Date of Response: (w/in 45 days of receipt of letter)</th>
<th>Result: (Access granted/Copies sent; Request denied; Hearing date; Records amended; Directory opt-out)</th>
<th>Handled by: (Name of Records Custodian)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following students have requested privacy holds for their directory information. This list should be reviewed before the school publishes students’ directory information in ANY manner, including in yearbooks, graduation programs, sports activity sheets, honor roll or other recognition lists, etc. The school MUST obtain written consent before publishing any of the following students’ information.

<table>
<thead>
<tr>
<th>Date Request was Received:</th>
<th>Student:</th>
<th>Contact Information for Obtaining Consent:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Bibliography & Additional Resources

The materials in the packet were adapted from and/or informed by the following resources & materials:

- United States Department of Education, Laws & Guidance, FERPA
- State of Hawaii, Department of Education, FERPA and Student Privacy
  - http://ferpa.k12.hi.us/IRM/FERPAWebsite.nsf/5cd7399be90745468a256c2c006ee384/1511d249ed9ec55b0a2575b8000053d4?OpenDocument
- Jordan School District, Planning and Student Services Manual:
- University of Tennessee Institute for Public Service, Country Technical Assistance Service: Student Records
  - https://ctas-eli.ctas.tennessee.edu/reference/student-records
Procedural Factors in Selecting a Hosting Service Provider
Technology has made it easier for educators to use data to make structural changes in education that will have a greater impact on more students. Many educators, at all levels, are outsourcing their schools’ IT departments to third-party hosting service data centers to achieve these goals, which often involves collecting and storing sensitive student data. While this collection student data is essential to the teaching and learning process, it must be done within parameters that protect the privacy of students and ensure that their data is used only for legitimate educational purposes.

The outsourcing of a school’s IT department presents multiple issues of transparency, privacy assurance, and efficient distribution of requested information. While the information collected by these agencies is generally described as “private,” removing the data from the school itself creates additional barriers in guaranteeing that the information is, in fact, private. As an initial matter, collection by third parties creates uncertainty as to what data, specifically, is catalogued. Moreover, how would a parent, for example, go about retrieving this information?

These uncertainties are relevant to virtually all actors in the school system. Therefore, in selecting a third-party hosting service provider, the administrators must be thorough and careful to ensure that they are making a well-informed and optimum choice for their specific goals. This reference sheet provides a checklist and explanation of relevant factors for school administrators to take into consideration when making a complete overhaul of their school’s IT department. The goal of this checklist is to ensure that administrators can make informed choices that protect the privacy of student data and facilitate FERPA compliance.

IN SELECTING A THIRD-PARTY HOSTING SERVICE PROVIDER,
EACH OF THE FOLLOWING CRITERIA IS MET:

Scope of the Product

☑️ Only data necessary for the services is shared
  
  To the extent that school resources allow, data should be minimized. This means that the school should share with the provider only the information that is absolutely necessary for the third-party to provide its services.

☑️ Data is stored securely
  
  The provider should ensure that data is stored securely so that the possibility of a breach is minimized. This means that the data is securely stored while it is being used and that it is properly erased when no longer used. To fully evaluate the technical requirements for a secure data storage system, see the Assessment Guide for Student Information Systems.

☑️ The school district retains control to review and amend data for errors and inaccuracies
  
  Where the data is collected for the benefit of the students and school, the school is in the best position to determine whether there are errors in the stored data. The school is also in the best position to ensure that the student data remains confidential. It is therefore important that the school be able to review the data collected. The school must retain control so that, if an error is detected, the school can readily correct that misinformation.

☑️ The education community is notified of the school’s use of an outside service provider
  
  In order to facilitate communication and understanding of all student data usage, school administrators should notify the parents which hosting service provider is used by the school selected.
Terms of Agreement

☑ The agreement states what data is being collected and how the provider will use the data
   The general purpose in using a third party hosting service provider is to securely provide the equipment and technological expertise to house the schools’ IT department. The terms of agreement should be clear in what data is kept and how that collection furthers the stated purpose(s).

☑ The agreement should allow parents to readily access their student's data through the provider or through the school
   FERPA requires that parents have access to their student data. Their support for a selected hosting service provider will stem from providing them with meaningful access to the data, in digestible form. The terms of agreement should thus permit parents to securely access their student’s data, either directly through the provider or readily through the school.

☑ The agreement delineates each party’s responsibilities in the event of a data breach
   While the selected product should be evaluated on its level of security, a leak of information is plausible at virtually any level of security. Therefore, it is important that, in addition to internal procedures within the school [see the Data Breach Response Plan], the provider and administrators come to an agreement on the responsibilities and procedures of each party should data be compromised.

☑ The agreement applies all relevant district rules
   State and district rules may have additional restrictions on student privacy. The terms of agreement should be in accord with any such rules.

☑ The agreement is reviewed by the central office and an attorney representing the school or school district
   The school's central office should be heavily involved in the process. The school or school district attorney should monitor the selection, including reviewing the terms of agreement, before a provider is selected.

Bibliography


Procedural Factors in Selecting a Data Analytics Service Provider
Technology has made it easier for educators to use data to make structural changes in education that will have a greater impact on more students. Many educators, at all levels, are utilizing third-party data analytics providers to achieve these goals, which often involves collecting and analyzing student data. While the collection and analysis of student data is essential to the teaching and learning process, it must be done within parameters that protect the privacy of students and ensure that their data is used only for legitimate educational purposes.

The use of third-party data analytics providers presents multiple issues of transparency, privacy assurance, and efficient distribution of requested information. While the information collected by these agencies is generally described as “private,” removing the data from the school itself creates additional barriers in guaranteeing that the information is, in fact, private. As an initial matter, collection by third parties creates uncertainty as to what data, specifically, is catalogued. How is that data stored, and for how long? How would a parent, for example, go about retrieving this information? Most importantly, what do the third-party data analytics service providers do with the data they collect?

These uncertainties are relevant to virtually all actors in the school system. Therefore, in selecting a third-party service provider, the administrators must be thorough and careful to ensure that they are making a well-informed and optimum choice for their specific goals. This reference sheet provides a checklist and explanation of relevant factors for school administrators to take into consideration when selecting a third-party service provider. The goal of this checklist is to ensure that administrators can make informed choices that protect the privacy of student data and facilitate FERPA compliance.

**IN SELECTING A THIRD-PARTY DATA ANALYTICS SERVICE PROVIDER, EACH OF THE FOLLOWING CRITERIA IS MET:**

**Scope of the Product**

- **Only data necessary for the services is shared**
  
  *To the extent that school resources allow, data should be minimized. This means that the school should share with the provider only the information that is absolutely necessary for the third-party to provide its services.*

- **Data is stored securely**
  
  *The provider should ensure that data is stored securely so that the possibility of a breach is minimized. This means that the data is securely stored while it is being used and that it is properly erased when no longer used. To fully evaluate the technical requirements for a secure data storage system, see the Assessment Guide for Student Information Systems.*

- **The educational resources provided are narrowly tailored to your students**
  
  *The services provided should not extend beyond the needs of the school. The product should be designed for the age and subject areas of students who are using it. Products that extend beyond the specific needs increase the risk that data collected for those purposes may be misused.*

- **The data collected is not directly associated with a student’s identity**
  
  *The collection of extensive, often longitudinal records raises macro-level concerns of subjecting a student to panoptic scrutiny. The provider’s method of collecting and processing data should ensure that raw data is not directly linked to the specific student. Where the nature of the service provided requires a direct link, that data is stored confidentially so that the linkage is minimal.*

© 2014 Lauren Irby. Prepared for Fordham University School of Law, Technology and Privacy Law (Fall 2014). These materials may be reproduced, in whole or in part, for educational and non-commercial purposes provided that attribute is included.
The education community is notified of the use of all outside service providers used by the school. In order to facilitate communication and understanding of all student data usage, school administrators should make available to parents a list of third-party service providers used by the school once those providers are selected.

The school district retains control to review and amend data for errors and inaccuracies. Where the data is collected for the benefit of the students and school, the school is in the best position to determine whether there are errors in the raw or processed data. The school is also in the best position to ensure that student data remains confidential. It is thus important that the school be able to review the data collected. The school must retain control so that, if an error is detected, the school can readily correct that misinformation.

Terms of Agreement

The agreement states what data is being collected and how the provider will use the data.
The general purpose in using a third party provider is to aggregate data to help identify student needs, monitor progression, and help students succeed. The terms of agreement should be clear in what data it collects and how that data furthers the stated purpose(s).

The agreement guarantees that the provider will not resell or otherwise disclose the data without parental consent.
It is important that student data be kept confidential. While FERPA does not apply to the third-party providers, the terms of agreement should reflect the restrictions of FERPA. Data should be treated as if it were held by the school itself, so that only those authorized under FERPA may access student information or authorize its use. The administrator should also consider whether to allow the provider to harvest the data for internal use, such as improving the product’s algorithms and design.

The agreement should allow parents to readily access their student’s data through the provider or through the school.
FERPA requires that parents have access to their student data. Parents are more concerned with their individual child’s progress than the overall progression of the school or other reports produced by the service provider. Their support for a selected data analytics provider will stem from providing them with meaningful access to the data, in digestible form, that will allow them to assess their child’s strengths and weaknesses. The terms of agreement should thus permit parents to securely access their student’s data, either directly through the provider or readily through the school.

The agreement delineates each party’s responsibilities in the event of a data breach.
While the selected product should be evaluated on its level of security, a leak of information is plausible at virtually any level of security. Therefore, it is important that, in addition to internal procedures within the school [see the Data Breach Response Plan], the provider and administrators come to an agreement on the responsibilities and procedures of each party should data be compromised.

The agreement applies all relevant district rules.
State and district rules may have additional restrictions on student privacy. The terms of agreement should be in accord with any such rules.

© 2014 Lauren Irby. Prepared for Fordham University School of Law, Technology and Privacy Law (Fall 2014). These materials may be reproduced, in whole or in part, for educational and non-commercial purposes provided that attribute is included.
The agreement is reviewed by the central office and an attorney representing the school or school district

The school’s central office should be heavily involved in the process. The school or school district attorney should monitor the selection, including reviewing the terms of agreement, before a provider is selected.

Education Community Involvement

A team of educators is involved in analyzing the data compiled

Data is often collected for the purpose of meeting standards set by governing bodies. Where a state/local agency evaluates a school’s growth, it is important that the school act as a mediator between the service provider and the evaluating body. An assigned team of educators, including administrators and teachers, should be involved in surveying the data collection and resulting reports to ensure that the process is fair and accurate.

Verifiable parental consent is provided for students using the product or service

The school district should demonstrate that it values and seeks parents’ consent by providing parents with notice and consent forms for their child’s involvement with the contracted service. The school should maintain organized documentation of parents’ consent.

Bibliography


Assessment Guide for Security of Student Information Systems
Assessment Guide for Security of Student Information Systems:

Instructions

This assessment tool is used to evaluate the data security of student information systems. The assessment tool provides questions and then explanations for those questions. Also included is a glossary of terms. Any word *highlighted* is defined in the glossary.

Most student information providers will store data at an off-site data center, so the questions below are worded with that in mind. However, it is possible that student information might be stored “locally.” This means that information about students will be kept on a computer (server) within your school district. Since the information will be stored on your Network, the security of student information will be partly dependent on your Network’s security. The questions below are just as applicable in that situation.

To use the tool, you should ask the sales team of a particular student information system the questions that are provided below. Along with the questions are explanations that explain why the questions are relevant, and what potential buzzwords may be in the student information system provider’s answer. For each question, you should assign a score based on the explanation below each question. In addition to the questions, a glossary of terms is provided. It is not necessary to utilize the glossary, but it is included if you are interested in learning more about certain data security technologies.

Encryption

1. **Will my students’ data be encrypted?**

   In the event that the security of your students’ information is breached, it is critical that the information is encrypted. Encrypted data is difficult, if not impossible, for an unauthorized user to read. Although FERPA does not clearly indicate that student data must be encrypted, encryption is vital to ensuring that student personal data is not accessed by unauthorized users.

   Award two points for encryption.

   If student data is left unencrypted, subtract a point.

2. **Will I access my students’ information over a secure connection?**

   It is not enough that students’ data is encrypted while it’s sitting on the server. In order to ensure that student data is protected, it is critical that when using the data, your connection to the server is secure. This may sound complicated, but all that is really needed is a little bit of technology to ensure that data remains encrypted as it travels back and forth. The service provider should at least mention using TLS or HTTPS.

   Award two points for use of TLS/HTTPS.

   If a secure connection is not used, subtract a point.
User Access Control

1. Does the student information system allow the creation of accounts that have access to differing amounts of data?

It is critical that the student information system has the ability to limit what material certain users have access to. It may be appropriate for certain users, like a building principal, to have access to all student data, whereas a parent should only be able to access information about their own children.

Award 2 points for a user access control system.

Data Segregation

2. Does your student information system use segregated data?

By using segregated data, the effects of a breach are minimized. For example, if information about a student’s special education status is stored separately from personally identifiable information, a partial breach is likely to be useless for an unauthorized user.

Award 1 point for segregation of data.

3. Will data unrelated to my school be stored on the same server?

The more individuals that have access to a server, the greater risk that the information stored on that server may be compromised. If only your school’s data is hosted on a server, it is easier to control the individuals that may have access to that data. This type of hosting arrangement is called a dedicated server.

Award 1 point for the use of a dedicated server.
Physical Security:

3. How physically secure is the data center site?

While the primary concern regarding the compromise of student data comes from cyber-attacks, it is also important that the data center is physically secure. The SANS Institute, a private company specializing in information security, provides a “Physical Security Checklist” for data centers. The best practices for physical security of a data center are:

• Require Photo ID for all data center employees.
• All employees at the facility should sign non-disclosure agreements.
• A perimeter fence that is twenty feet from the building, with guard kiosks at each access point.
• Security Cameras both outside the data center and within the data center.

Award 1 point for addressing 3 or 4 of the physical security best practices.
Award half a point for addressing 2 of the physical security best practices.
Award no points for addressing 1 of the physical security best practices

Data Center Auditing

4. Has the data center been audited?

There are a variety of audit standards that data centers may choose to comply with. It would be prudent for any data center hosting student information to at least meet the standard for a HIPAA audit. HIPAA is a federal privacy statute that protects the privacy of medical records. A HIPAA audit determines if a data center has the proper policies and protections to ensure that medical records are not compromised.

Another audit standard is the PCI DSS. This security audit ensures that a data center has the proper policies and protections to store credit card holder data.

Award 2 points for a HIPPA audit or PCI DSS audit.
Award 1 point for compliance with any other audit standard.
Data Security Rubric

<table>
<thead>
<tr>
<th>Service Provider Name:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Category:</strong></td>
<td><strong>Score:</strong></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td><strong>Encryption</strong>&lt;br&gt;Question 1: Hard Disk Encryption&lt;br&gt;Question 2: Transmission Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User Access Control</strong>&lt;br&gt;Question 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Segregation of Information</strong>&lt;br&gt;Question 4: Segregated Data&lt;br&gt;Question 5: Segregated Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical Security</strong>&lt;br&gt;Question 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Center Auditing</strong>&lt;br&gt;Question 7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Score:  /11
Glossary of Terms

**Firewall** – A firewall controls network traffic by filtering what is allowed in and out based on a security policy. A firewall is like a security guard controlling who can enter and exit a building.

**Encryption** – Encryption is the process of storing data in a way that cannot be read by unauthorized users. The technical term for this type of data is “ciphertext.” It is similar to creating a coded message an individual could only read if they knew the code.

**Data Center** – A data center is essentially a building full of computers. Service providers often store information on computers that are housed within data centers.

**Server** – A server is a type of computer. Servers often store information, and make that information available to users.

**Network** – A network is a group of computers.

**Transport Layer Security (TLS)** – TLS is a way of securing communications on the internet. This technology attempts to limit unauthorized users’ ability to “eavesdrop.”

**HTTPS** – HTTPS provides a way to encrypt the normal day-to-day communications on the web. Typically, when a webpage is employing HTTPS, a lock symbol appears in the address line.

**Segregated Data** – Data segregation is a technique where information is physically stored in different places. It would be the equivalent of storing the combination to a safe in a location separate from the safe.

**Personolly Identifiable Information** – Personally Identifiable Information is any information that can identify a particular student.
Bibliography

CHARLIE KAUFMAN ET AL., NETWORK SECURITY: PRIVATE COMMUNICATION IN A PUBLIC WORLD (2d Ed. 2002).


Data Breach Response Plan
DATA BREACH RESPONSE PLAN

Data breaches are real and inevitable. It is important to be prepared, act quickly, and prevent further disclosure of data. Below are guidelines for responding to a reported or suspected data breach. Note: Many response activities occur simultaneously. Address the immediate response activities first, but review the entire checklist to determine which steps may be relevant to you as the situation unfolds.

Immediate Response

- Appoint a senior administrator as incident manager, who will oversee the situation and response.
- Attempt to identify the source of the breach; examples include hacking, lost or stolen equipment, weak security policy, or staff negligence.
- If computers or other devices were lost, stolen, or hacked, disable all user accounts connected to that device. If possible, attempt to recover or remotely wipe the device.
- If the breach occurred at an offsite vendor or service provider, contact the vendor to discuss mitigation efforts and affected data.
- Review any access logs to the network, programs, and accounts beginning when the breach occurred. Determine if data was accessed, and what data is at risk.
- Immediately request all affected staff to change their account and device passwords.
- Contact your legal counsel.

Secondary Response

Communication:

- If you suspect that criminal activity was involved, contact law enforcement.
- Establish a communication plan to manage public messages about the breach.
  - Advise all staff not to disclose any details until further notice.
  - Prepare a statement or press release in the event the media becomes aware of the breach.
- Contact vendors or service providers who may have contributed to or been affected by the breach.
- Review your state breach notification law, if any, and determine whether any official notices need to be issued and to whom. If notices are not required by law, consider whether it would be advisable to provide notices anyway.
- Record all information relevant to the breach and document all response and reporting efforts.

Investigation:

- Determine whether the investigation will be handled internally or if it will be outsourced to a specialized incident response firm.
- Interview staff and review any access logs and records.
- Identify what information was disclosed and which individuals were affected.
- Identify any affected computers, devices, or other equipment.
Recovery:

- Determine who will review the response efforts and make adjustments for the future.
- Review access controls and procedures to identify and resolve any weaknesses.
- Determine whether revisions are required to current data and security policies and procedures.
- Review contracts with vendors or service providers. Consider revising contracts to include breach notification, security requirements, and insurance or compensation for any future incidents.

Bibliography and Resources

Technology Security Checklist for Teachers
TECHNOLOGY SECURITY CHECKLIST FOR TEACHERS

Technology has an increasing presence in schools and classrooms. However, these tools also pose security risks to sensitive data. Teachers play an important role in protecting student privacy. Below is a checklist of security procedures to follow when using school-related technology.

General Guidelines

- Do not share passwords for school accounts with anyone, including other staff or family members.
- Use different passwords for your school accounts than you do for personal accounts.
- Avoid connecting to the Internet through wireless networks (WiFi) that are not password protected.
- Immediately report to the administration any suspicious activity involving or affecting technology related to school work, school accounts, or student data.

Using Computers, Tablets, and Other Devices

When you are using school-owned equipment:

- Ask the administration whether your district or school has a policy about using school-owned computers, tablets, or other devices.
- Log out of accounts and close browsers and programs whenever you finish using a program.
- Password-protect, lock, or otherwise secure all computers and devices when not in use.
- Immediately report lost or stolen devices to the administration.

When you are using your own equipment:

- Ask the administration whether your district or school has a policy about bringing your own computer, tablet, or other device to school or using your own device for school purposes.
- Ask the administration if approval is necessary prior to using your own computer or other device in the classroom or to access student data.
- Install anti-virus software on the device before using it on the school network or to access school accounts; below are links to free anti-virus programs available for download:
  - Avast Free Antivirus: http://www.avast.com/index
- If the device or a program notifies you that critical security updates or patches are available, promptly follow the instructions on the screen to download and install the updates.
- Set up password protection to log in to the device, wake the device, or unlock the screen; below are links to webpages with password how-to guides:
  - Chrome OS: https://support.google.com/chromebook/answer/2587994?hl=en
  - iPhone/iPad: http://support.apple.com/en-us/ht4113
  - Android: https://support.google.com/playedition/answer/2819522?hl=en

© 2014 Elizabeth Walker. Prepared for Fordham University School of Law, Technology and Privacy Law (Fall 2014).
Log out of accounts and close browsers and programs whenever you are finished.
Password-protect, lock, or otherwise secure all computers and devices when not in use.
Immediately report lost or stolen devices to the administration.

Choosing Software and Web Applications
- Ask the administration whether your district or school has a policy about choosing software and web applications that may be used in the classroom or for other school purposes.
- Ask the administration if approval is necessary before downloading and using any software or web applications.
- Try all programs prior to inputting student data or using the program in the classroom.
- Consider whether the program requires you to enter student data or excessive information as a condition to use the program.
- Look for any advertisements displayed in the program, which may be a sign the program shares data with third parties.
- Analyze whether the program utilizes any security protocols, such as password protection or the web address includes the words “https” and a padlock symbol similar to this image:
- Avoid using any programs that appear to be suspicious.

Using Email
- Ask the administration whether your district or school has a policy about using email.
- Do not click on any links or download any attachments you receive from a suspicious source.
- Be cautious of emails containing the following:
  - Links in suspicious-looking messages
  - Threats that your account will be closed if you do not respond
  - Web addresses where names of well-known companies have been slightly altered
  - Requests for personal information
  - Unexpected attachments, especially those purporting to come from banks or financial institutions
  - Deals that sound too good to be true
  - Urgent emails demanding that you act immediately
  - Messages that list your email as the sender or from address

Accessing or Sharing Student Data
- Ask the administration whether your district or school has a policy about using or sharing student data.
- Only access the student data that you have permission to access.
- Only access student data for legitimate school or educational purposes.
When accessing student data, only use computers or devices that have either been approved by the school or that contain security software and are password protected.

- Lock up hardcopy files and devices with access to student data.
- Do not share or disclose student data without authorization from an administrator, parent, or guardian.
- Do not share student data during public meetings or presentations; use fictitious records instead.
- Avoid sending student data via email unless specifically authorized.
- Immediately report any incidents to the administration where you believe student data may have been inappropriately accessed or shared.

Bibliography and Resources

- Colorado Department of Education, Data-Sharing & Confidentiality Agreement: http://www.cde.state.co.us/cdereval/cdeemployeedatasharingconfidentialityagreement

OVERVIEW

I. What is FERPA?
II. What rights does FERPA provide?
III. What information does FERPA protect?
IV. How does FERPA affect my classroom?
V. FERPA Scenarios ➔ Assessment

WHAT IS FERPA?
THE BASICS

In this section:
- What is FERPA?
- Who is granted rights under FERPA?
- Who enforces FERPA?
- Is my school subject to FERPA?
WHAT IS “FERPA?”

FERPA = FAMILY EDUCATIONAL RIGHTS & PRIVACY ACT

THE BASICS

What is FERPA?

- FERPA is a federal law that protects the confidentiality of student education records.
- FERPA is a federal law, found in Title 20 of the United States Code. The federal regulations are found in Title 34 of the Code of Federal Regulations.
- Both the text of the law and its regulations are helpful to understand how to comply!

THE BASICS

Who is granted rights under FERPA?

- Parents are granted rights, on behalf of their children.
- Rights transfer to students when they turn 18 years old OR attend a postsecondary institution (“eligible students”), but...
- Parents who claim children as dependents on their taxes retain their rights.
THE BASICS

Who enforces FERPA?

- FERPA is administered by the Family Policy Compliance Office (FPCO) in the Department of Education.
- If a parent or eligible student files a FERPA complaint against your school, the FPCO may investigate your school’s procedures to determine what action should be taken.

THE BASICS

Is my school subject to FERPA?

- FERPA applies to all schools that receive federal funding for any program administered by the Dept. of Education.

WHAT RIGHTS DOES FERPA PROVIDE?

A GUIDE TO FERPA’S ESSENTIAL REQUIREMENTS

In this section...
- Rights granted under FERPA
- Your school’s obligations to ensure these rights
WHAT RIGHTS DOES FERPA PROVIDE?

FERPA gives parents (and eligible students) the right to:

1. Prevent the disclosure of personally identifiable information from their education records without consent;
2. Access to review and inspect student education records; and
3. Request correction of these education records.

WHAT INFORMATION DOES FERPA PROTECT?

In this section...
- What are “education records”?
- What is “directory information”?
- What should you know about disclosing student information?

FERPA prevents disclosure of information from a student’s “education record,” but does not prevent disclosure of “directory information.”
EDUCATION RECORDS are...

Records directly related to a student that are
• maintained by the school, or
• maintained by a third-party vendor, on behalf of the school.

FERPA prohibits release of education records without consent of parents or the eligible student.

EXAMPLES OF EDUCATION RECORD INFORMATION:

• Student grades
• Immunization & health records maintained by the school
• Disciplinary records
• Student progress reports
• Academic or physical testing results
• Grade point average
• Attendance records

You MUST keep information in a student’s education record confidential and secure.

WHAT IS NOT PART OF AN “EDUCATION RECORD”

• Private records a teacher makes during the course of teaching, meant for the teacher’s private use as a memory aid
• Law enforcement or campus security records created and maintained solely for law enforcement reasons.
• Employment records (unless employment is contingent upon enrollment and attendance)
• Alumni records
• Grades on peer-graded papers before they’re recorded
**“EDUCATION RECORDS”**

**KNOWLEDGE CHECK: Education Record? Yes or No**

- Log of student’s disciplinary history: Yes
- Student’s health records created by school nurse: Yes
- Teacher’s written notes for own use: No
- Records kept by campus security re: vandalism incident: No
- Teacher’s gradebook: Yes
- Student transcript: Yes

Confused? Talk to your colleagues, supervisors, and administrators. Always ASK if you’re unsure before disclosing information!

---

**WHAT INFORMATION IS PROTECTED UNDER FERPA?**

**Scenario**

As you’re walking back to your classroom from lunch, you notice a couple of students fighting in the hall. Your knowledge of the events comes only from this direct observation.

*Does FERPA govern disclosure of what he or she saw?*

---

**WHAT INFORMATION IS PROTECTED UNDER FERPA?**

**ANSWER**

_No_, FERPA does _not_ prohibit a school official (here, the teacher) from disclosing information he or she witnessed. Direct observations are _not_ part of a student’s education record.

- A school official _may_ disclose what he or she saw or overheard to appropriate authorities, including administrators, other school officials, parents, or law enforcement.
PERSONALLY IDENTIFIABLE INFORMATION

Information that, alone or in combination, would generally allow a person in the school community to identify a student with reasonable certainty.

FERPA prohibits the release of “personally identifiable information” contained in a student's education record, unless it is directory information...

DIRECTORY INFORMATION is...

Personally identifiable information that is not generally considered harmful if disclosed (i.e. basic information).

- FERPA allows schools to disclose this information without consent, as long as they provide public notice to families that explains what types of information the school has designated as “directory information.”

COMMON EXAMPLES OF “DIRECTORY INFORMATION”

- student’s name
- address
- telephone number
- date of birth
- major field of study
- participation in officially recognized activities/sports
- weight & height of athletic team members
- dates of attendance
- degrees/awards received
- most recent previous educational institution attended by student
- e-mail address
- place of birth
- photograph
- grade level
- enrollment status
A RECAP: WHAT INFORMATION DOES FERPA PROTECT?

**EDUCATION RECORDS**
Information directly related to a student and that is maintained by the school, or a party acting on the school’s behalf.

**DIRECTORY INFORMATION**
- Information about a student, defined by the school through notice to parents and eligible students.
- Information that would not generally be considered harmful if an invasion of privacy occurred.

**MAY**
be disclosed without consent

**MAY NOT**
be disclosed without consent.

But, there are some special circumstances that allow disclosure of education records without consent...

DISCLOSURES

REMEMBER
Assume all information directly related to a student is part of that student’s education record and therefore cannot be disclosed without written consent, but, FERPA allows a few specific exceptions...

SPECIAL CIRCUMSTANCES for DISCLOSURE OF EDUCATION RECORDS

To other school officials with “legitimate educational interest”
- Ex.: other educators, academic coaches, or tutors

To appropriate officials in health/safety emergencies
- Use your judgment — your students’ safety is the priority, and FERPA allows for necessary disclosures in times of emergencies.
- Ex.: sharing student allergies with paramedics if a student is in shock.

Talk to your administrator!
FERPA permits a few other disclosures, however, it is unlikely you will encounter these in a classroom. If you are asked to share protected information that seems reasonable to disclose, ask for advice first.
HOW DOES FERPA IMPACT MY CLASSROOM?

1. Be careful with the technology you use in your lessons.
   - Don’t use websites that require your students to enter personal information unless it has been approved by a supervisor or your school’s technology officer.
   - Find out what companies or vendors your school is either working with or feels comfortable working with.
   - Continue to evaluate the technology you and your students utilize.

2. Keep any student data you have secure.
   - Store your students’ data and information using your schools’ data management systems.
   - Don’t email information to unverified parent email addresses – be sure you’re not accidentally disclosing student information to the wrong people.
   - Keep any physical graded materials or grade books in secure, safe places.
   - Don’t discuss student information with others, unless that person has a “legitimate educational goal.”
HOW DOES FERPA IMPACT MY CLASSROOM?

3. Responding to access requests:
   • You may communicate education record information with students’ parents.
   • Be sure you know your students’ legal guardians: under FERPA, “parent” includes “a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or guardian.”
   • If you ever receive a request to inspect or review education records you do not have access to, tell your administrator.

FERPA SCENARIOS

The following slides contain different scenarios that will test your knowledge of FERPA’s requirements. Discussing these scenarios and learning from the answers may help to clarify any questions you still have regarding FERPA.

SCENARIO 1

You leave your room for a few minutes during your planning time. Before you left you were working with personal student information but you did not lock your computer. While you were gone, an unauthorized person came by your room and retrieved some student information from the computer screen.

Under FERPA, is your school responsible?
SCENARIO 1 – ANSWER

Information on a computer screen should be protected the same way as printed reports. Computer programs with confidential information should be closed when you are not using them, and computers should be locked when you leave the room. Printed materials should be filed in a secure place, and not simply left out on a desk.

The medium that holds the information is not important under FERPA laws – no information should be left accessible or unattended, including computer screens.

SCENARIO 2

Skipping class has become a problem at your school. Your principal and local police have been looking for students who are not in school during the day. You receive a phone call from the local police asking if a particular student was in attendance in your class yesterday. They tell you that they are investigating whether the students were involved in some vandalism and need to know their whereabouts.

Can you give them the information?

SCENARIO 2 – ANSWER

You cannot give the attendance information to the police department. Attendance records are considered part of the students’ educational record and cannot be released without consent of the parents or eligible student.

Unless the police have obtained legal authority to compel you to disclose the information, it would be a violation of FERPA to share part of the student’s educational record.

...If, however, the information was related to a health or safety emergency, or attendance records are designated by your school as directory information, then the information could be disclosed without consent!
SCENARIO 3

During class, you receive a message that the father of one of your students has called for you. You call him back after school and he tells you he is just curious how his 11 year old daughter is doing in class. He would like to check that her attendance and grades are still strong.

Can you give them this information over the phone?

SCENARIO 3 – ANSWER

Your school should have a way to attempt to verify that the person you’re calling is, in fact, the parent. Once verified (maybe you have saved the parent’s phone number, for example), then yes, you can discuss this information with them.

SCENARIO 4

A parent comes into your room one day after school. Her daughter’s birthday is next week and she would like to have a list of students’ names in the class and their addresses to send out invitations to the birthday party. You have known this parent for years and trust her.

Can you provide her with the names and addresses of the students in the class?
SCENARIO 4 – ANSWER

Each school district is required to identify the categories of information that they consider to be directory information. As long as the school has given parents and eligible students annual notice, the information the mother seeks may be categorized as directory information and would be acceptable to disclose. If, however, your school has not designated this information as directory information, you may not disclose it.

APPENDIX
HELPFUL MATERIALS AND LINKS

GLOSSARY

Directory Information: information designated by a school that is more basic and is not harmful if disclosed.
Education Records: records maintained by the school that are directly related to a student
Eligible Student: A student who is either 18 years of age or older, or is attending a post-secondary institution.
FERPA: Family Educational Rights & Privacy Act, federal law that governs confidentiality of student educational records.
FPCO: Family Policy Compliance Office, enforces FERPA.
Personally Identifiable Information: contains information that would make the student’s identity and any related information about him or her easily recognized.
LINKS TO HELPFUL BACKGROUND INFORMATION

FERPA STATUTE AND REGULATIONS
Full Text of FERPA - Cornell Law Website
FERPA Federal Regulations - Cornell Law Website

OTHER MATERIALS
- FPCO Website for Parents
- FPCO PDF for Parents – February 2011
- FPCO Guidance for Parents – October 2007
- National Center for Education Statistics - Resources for FERPA Access
- PTAC Disclosure Exceptions Rubric

BIBLIOGRAPHY
This presentation was created using materials from the following institutions:
- The Family Policy Compliance Office (FPCO)
- Data for Student Success (Data4SS.org)
- Skyline High School, Ann Arbor, MI
- Cornell University Law School
- National Center for Education Statistics (NCES)
Professional Development Training Materials – FERPA FAQs
FERPA’s FREQUENTLY ASKED QUESTIONS

1. **What is FERPA?**

FERPA, the Family Educational Rights and Privacy Act, is a federal law that affords parents the right to: 1) have access to their children’s education records; 2) the right to seek to have the records corrected or amended, and; 3) the right to have some control over the disclosure of personally identifiable information from the education records.

When a student turns 18 years old or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student").

The FERPA statute is part of the United States Code, and is found at 20 U.S.C. § 1232g. FERPA regulations are in the Code of Federal Regulations, and are found at 34 CFR Part 99.

2. **What is “Directory Information”?**

FERPA defines "directory information" as information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed.

Typically, "directory information" includes information such as name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance.

A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information."
3. WHAT ARE THE REQUIREMENTS OF A SCHOOL’S ANNUAL FERPA NOTICE?

Schools may send notice of FERPA rights any way that is “reasonably likely to inform the parents or eligible students of their rights.” There is no “correct” method – a school may choose to send the notice in a letter, include a provision in a student handbook, add a FERPA-rights section to ‘back-to-school’ materials, or by other reasonable means.

This notice must inform parents and eligible students that they have the right to—

i. Inspect and review the student’s education records;

ii. Seek amendment of education records they believe are inaccurate or misleading;

iii. Consent (or refuse to consent) to disclosures of personally identifiable information; and

iv. File a complaint with the Department of Education concerning possible failures of the school to comply with FERPA.

Additionally, if a school plans to disclose “directory information,” it must give notice of:

i. The types of personally identifiable information that the school has designated as directory information;

ii. A parent’s or eligible student’s right to refuse to let the school designate any or all of those types of information about the student as directory information; and

iii. The period of time within which a parent or eligible student must notify the agency or institution in writing that he or she does not want any or all of these types of information about the student designated as directory information.

4. UNDER WHAT CIRCUMSTANCES MAY A SCHOOL DISCLOSE INFORMATION FROM EDUCATION RECORDS WITHOUT CONSENT?

FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions:

• School officials with legitimate educational interests;

• School to which student is transferring;

• Specified officials for audit or evaluation purposes;

• Appropriate parties in connection with financial aid to a student;

• Organizations conducting certain studies for or on behalf of the school;

• Accrediting organizations;

• To comply with judicial orders or subpoenas;

• Appropriate officials in health/safety emergencies;

• State and local authorities pursuant to specific State law.

However, other than in these instances, schools need written permission from the parent or eligible student in order to release any information from a student’s education record.
5. WHAT SHOULD A SCHOOL DO WHEN PARENT OR ELIGIBLE STUDENT REFUSES TO DESIGNATE INFORMATION AS “DIRECTORY INFORMATION”?

A parent or eligible student, upon receiving notice of the school’s designated categories of directory information, may wish for any or all of that information not to be designated as the student’s directory information.

If so, the school must ensure that any disclosures of this information that it makes (on athletic rosters, to local newspapers, etc.) do not include any of the refused information for this student.

6. HOW ARE DISCIPLINARY RECORDS DIFFERENT FROM “LAW ENFORCEMENT RECORDS”?

Disciplinary records are records about a student’s behavior regarding school policies and procedures. For instance, fighting with another student in the hallway is almost certainly against your school’s rules. If a staff member sees this behavior and assigns the student detention, that may enter the child’s disciplinary record. These records are part of the student’s education record.

“Law enforcement records” are records created by law enforcement units for law enforcement purposes. If your school employs security guards who patrol campus grounds, and catches two students vandalizing the property, law enforcement officer may record the information, which is for a law enforcement purpose. This information is not part of the student’s education record.

7. IF PROVIDING ACCESS TO EDUCATION RECORDS IS NOT FEASIBLE, WHAT PROCEDURES MUST MY SCHOOL FOLLOW?

If circumstances prevent the parent or eligible student from being able to inspect and review education records, the school must either:

1. Provide the parent or eligible student with a copy of the records requested; or
2. Make other arrangements for the parent or eligible student to inspect and review the records.

The school may charge a fee if it provides a copy of the records, unless the fee would prevent the parent or eligible student from being able to inspect and review the records. (A small, administrative fee to cover the cost of the paper and ink is typically all right.) Also, the school may not charge a fee to search for or retrieve education the records of a student.

8. HOW MUST A SCHOOL ADDRESS REQUESTS TO AMEND OR CORRECT EDUCATION RECORDS?

First, if a parent or student believes part of the student’s education record is inaccurate, missing, misleading, or in violation of the student’s rights of privacy, he or she may ask the school to amend the record. Once the school receives the request, a school officer should determine whether to amend the record or not “within a reasonable time.” Then, if the school decides not to amend the record as requested, the school must inform the parent or eligible student to his or her right to a hearing.
If, after the hearing, the school decides the information should be changed, it must:
1. Amend the record accordingly; and
2. Inform the parent or eligible student of the amendment in writing.

If, however, the school’s opinion does not change after the hearing, the school must:
1. Inform the parent or eligible student of the right to place a statement in the record with his or her own view of the matter;
2. Maintain this included statement with the contest part of the record for as long as the record is maintained; and
3. Disclose the statement whenever it discloses the portion of the record to which the statement relates.

9. WHY ARE A TEACHER’S PERSONAL NOTES NOT INCLUDED IN A STUDENT’S EDUCATION RECORD, BUT THE TEACHER’S GRADE BOOK IS INCLUDED?

FERPA makes an exception to the “education record” information by eliminating the notes a teacher takes, for memory reasons, that are intended to remain in the sole possession of the teacher – which is great, because teachers jot down notes all the time! If these notes were part of a student’s education record, then gaining access to them or seeking to amend them would be very burdensome and impractical. Therefore, FERPA does not include the notes a teacher takes, for his or her use only, as part of the education record.

A teacher’s grade book is a different story. The records in a grade book are often used to calculate a student’s final grades, which are counted in the education record. FERPA only allows this exception to extend to the teacher’s personal, private notes taken as an aid; a grade book does not qualify and it is part of the education record.

10. IF THE SCHOOL HAS STUDENTS WHO ARE 18 YEARS OR OLDER, MUST IT RESPOND TO ACCESS REQUEST FROM THEIR PARENTS?

The rights under FERPA transfer from the parents to the student, once the student turns 18 years old or enters a postsecondary institution at any age. However, although the rights under FERPA have now transferred to the student, a school may disclose information from an “eligible student’s” education records to the parents of the student, without the student’s consent, if the student is a dependent for tax purposes. Neither the age of the student nor the parent’s status as a custodial parent is relevant. If a student is claimed as a dependent by either parent for tax purposes, then either parent may have access under this provision.

In this instance, the student and the parents would have FERPA rights.
Bibliography

This FAQ page was adapted from the following FPCO materials:

FERPA is a federal law that requires confidentiality of student information by telling schools what information it may share, and when & who they may share such information with. It also gives parents the right to consent to the disclosure of their child’s personally identifiable information (“PII”).

**Educational records** are records directly relating to a student that are maintained by the school or by a third party that the school enlists for certain functions.

> For example, a company that provides you with course management software.

**Directory information** is educational records that are generally not considered harmful to students if publicly released, such as name, age, address, and grade level.

> PII can be either directory information or non-directory information.

**Non-directory information** is educational records that are more sensitive than directory information, such as social security & student ID numbers, grades, disciplinary history, and attendance record.

Under FERPA, you cannot share non-directory, PII information without parental consent. Generally, you can share directory information without parental consent, unless parents have told the school otherwise. So, think carefully about whether an activity, like an online assignment submission program, means sharing student information without parental consent. On the back page is a list of Do’s and Don’ts for some routine classroom activities.
## FERPA Dos & Don’ts

<table>
<thead>
<tr>
<th>Do’s</th>
<th>Don’ts</th>
</tr>
</thead>
</table>
| • **DO** ask yourself:  
  • Am I sharing student information?  
  • Can someone personally identify my student from this information?  
  • Do I have parental consent?  
  • **DO** check your school’s annual FERPA notice to see which educational records it has designated as directory information.  
  • **DO** check with the administration office to see if any parents have told the school not to share their child’s directory information.  
  • **DO** shred student documents before disposal.  
  • **DO** use educational technology pre-approved by your school.  
  • **DO** check for parental consent before including non-directory information in a student recommendation. | • **DON’T** use educational technology programs that your school does not have a contract for. Check with your school administration if you are unsure whether a contract exists for a particular program.  
  • **DON’T** send student grades and other non-directory information via e-mail – if parents ask for their child’s grades, pick up the phone instead!  
  • **DON’T** publicly post students’ personal information online without parental consent.  
  • **DON’T** use social networks to connect students with classroom pages and events without parental consent. |

### Tips

Records that you keep for your own personal memory aid and are for your eyes only, like classroom notes, are **not** subject to FERPA.

You may disclose non-directory information in an emergency. That is, when it is necessary to protect the health and safety of student(s).

For additional FERPA resources, visit [www2.ed.gov/fpco](http://www2.ed.gov/fpco) and [http://ferpasherpa.org/](http://ferpasherpa.org/).
Bibliography & Additional Resources

The materials in the packet were adapted from and/or informed by the following resources & materials:

**U.S. Department of Education, Laws & Guidance, FERPA**

**Consortium for School Networking (CoSN)**
http://www.cosn.org/focus-areas leadership-vision/protecting-privacy

**FERPA|SHERPA**
http://ferpasherpa.org/p-s.html
FERPA is a federal law that requires confidentiality of student information and protects student privacy by giving parents several important rights regarding their child’s educational records.

**Educational records** are information directly relating to a student and maintained by the school, such as grades, standardized test scores, attendance, disciplinary history, and special needs history.

FERPA provides parents three important rights:

<table>
<thead>
<tr>
<th>Access Right</th>
<th>Correction Right</th>
<th>Opt-Out Right</th>
</tr>
</thead>
<tbody>
<tr>
<td>This right allows parents to inspect their child’s educational records held by a school district. This is an important right because it allows parents to see what information a school is collecting and whether that information is accurate.</td>
<td>This right allows parents to request an amendment to their child’s educational records if they feel the records are inaccurate, misleading, or a violation of privacy. This is an important right because children’s educational records could affect their future, such as with college admissions or special needs placement.</td>
<td>This right allows parents to opt-out of schools sharing directory information in most circumstances with third parties. A school may share this info until it receives a written opt-out notice from a parent. This is an important right because some third parties may use this information to personally identify you or your child in order to market goods and services.</td>
</tr>
</tbody>
</table>

**Directory information** is a type of educational record that may include your child’s name, address, telephone number, birth date, height, weight, and participation in official school extracurricular activities. Under FERPA, a school must tell parents each year what it classifies as directory information.
Exercising Your FERPA Rights

Call the principal’s office to find out the name and contact information of the school’s records custodian.

Write a letter to the records custodian. Check below to see what you should include in your letter.

Tip! Always include your child’s name, your name, and your contact information for how & where the records custodian can best reach you.

Access Right

If you wish to inspect your child’s records, your letter should include:

- Statement that you are requesting to inspect and review your child’s records under FERPA
- A request that the records custodian send you a copy of your child’s educational records.* Note that the records custodian must respond within 45 days of your request

*Instead of sending you a copy, some schools may set up a time and place for you to inspect the records in person

Correction Right

If you believe your child’s educational records are inaccurate, misleading, or a violation of privacy, you may seek to amend these records. You cannot amend a grade, opinion, or substantive decision made about your child. Your letter should include:

- The record(s) you are seeking to amend
- The reason you are seeking to amend the record(s)
- How the record(s) should be amended

Opt-Out Right

If you do not want your child’s directory information to be shared with third parties (in most circumstances), your letter should include:

- Statement that you do not consent to the disclosure of your child’s directory information

Schools may provide an opt-out form or set an opt-out notice deadline each year. Call the principal’s office to find out if there is a required form or a deadline date!

A school may reject your amendment request, but you will have a right to a hearing, where a decision will be made based solely on the evidence provided at the hearing. If the rejection is upheld at the hearing, you may insert a statement in the records explaining why you believe the records to be inaccurate, misleading, or a violation of privacy.
FERPA is a federal law that requires confidentiality of student information and protects student privacy by giving students 18 years and older several important rights regarding their educational records.

Educational records are information directly relating to a student and maintained by the school, such as grades, standardized test scores, attendance, disciplinary history, and special needs history.

FERPA provides adult students three important rights

**Access Right**
This right allows adult students to inspect their educational records held by a school district. This is an important right because it allows adult students to see what information a school is collecting about them and whether that information is accurate.

**Correction Right**
This right allows adult students to request an amendment to their educational records if they feel the records are inaccurate, misleading, or a violation of privacy. This is an important right because students’ educational records could affect their future, such as with college admissions or special needs placement.

**Opt-Out Right**
This right allows adult students to opt-out of schools sharing directory information in most circumstances with third parties. A school may share this info until it receives a written opt-out notice from the adult student. This is an important right because some third parties may use this information to personally identify the adult student in order to market goods and services.

Directory information is a type of educational record that may include a student’s name, address, telephone number, birth date, height, weight, and participation in official school extracurricular activities. Under FERPA, a school must tell adult students each year what it classifies as directory information.
Exercising Your FERPA Rights

Call the principal’s office to find out the name and contact information of your school’s records custodian.

Write a letter to the records custodian. Check below to see what you should include in your letter.

*Tip! Always include your name and your contact information for how & where the records custodian can best reach you.*

### Access Right
If you wish to inspect your educational records, your letter should include:
- Statement that you are requesting to inspect and review your educational records under FERPA
- A request that the records custodian send you a copy of your educational records.*

Note that the records custodian must respond within 45 days of your request.

*Instead of sending you a copy, some schools may set up a time and place for you to inspect the records in person.

### Correction Right
If you believe your educational records are inaccurate, misleading, or a violation of privacy, you may seek to amend these records. You cannot amend a grade, opinion, or substantive decision made about you. Your letter should include:
- The record(s) you are seeking to amend
- The reason you are seeking to amend the record(s)
- How the record(s) should be amended

### Opt-Out Right
If you do not want your directory information to be shared with third parties (in most circumstances), your letter should include:
- Statement that you do not consent to the disclosure of your directory information

Schools may provide an opt-out form or set an opt-out notice deadline each year. Call the principal’s office to find out if there is a required form or a deadline date!

A school may reject your amendment request, but you will have a right to a hearing, where a decision will be made based solely on the evidence provided at the hearing. If the rejection is upheld at the hearing, you may insert a statement in the records explaining why you believe the records to be inaccurate, misleading, or a violation of privacy.
The materials in the packet were adapted from and/or informed by the following resources & materials:

- U.S. Department of Education, Laws & Guidance, FERPA
- Consortium for School Networking (CoSN)
  - http://www.cosn.org/focus-areas/leadership-vision/protecting-privacy
- FERPA|SHERPA
  - http://ferpasherpa.org/p-s.html