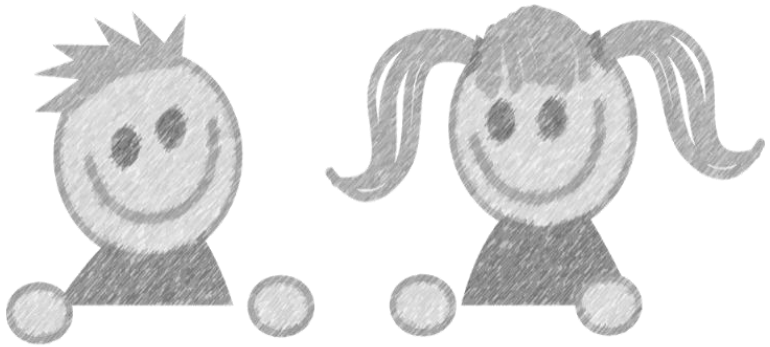
West Virginia DEPARTMENT OF EDUCATION

FERPA for Counselors: Confidentiality Day-to-Day

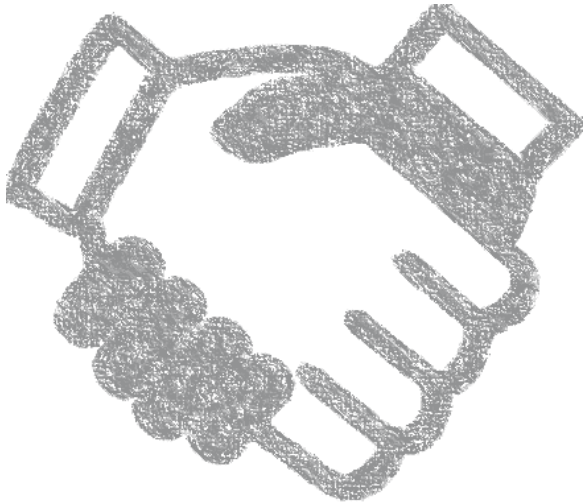
Understanding FERPA to Keep Your Students Safe

March 2020

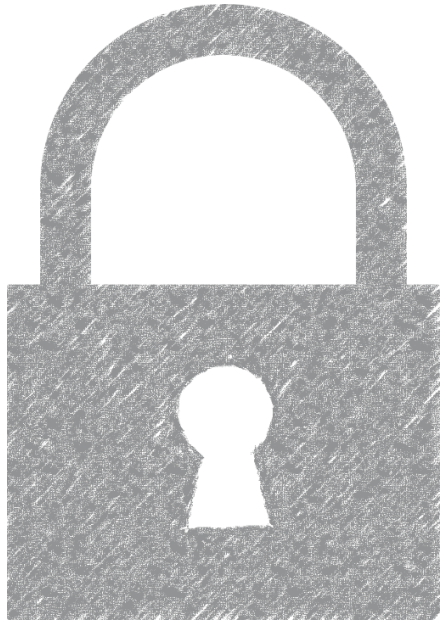
Remember



Respect



Protect



Privacy Foundations

Regulations lay the groundwork for protecting privacy

Education Privacy Regulations

- FERPA (Family Educational Rights and Privacy Act)
- Student DATA Act (W. Va. Code §18-2-5h)
- WVBE Policies (4350, 2315)
- Local Policies
- Other federal & state law
- **American School Counselor Association Ethical Standards**

FERPA Foundations

- Born: 1974
- Found at: 34 CFR Part 99
- Applies to: Schools accepting funds from U.S. Department of Education
- About: Privacy and confidentiality, parent and student rights, education agency roles and responsibilities

FERPA Foundations

- Data must be protected.
- Parents and students have rights.
- Data decisions are local.
- Tell people what's going on.
- You need to have a need for it.
- Get permission beforehand.
- Share with care.

FERPA Foundations

- Education Record
- Personally Identifiable Information (PII)
- Access and Disclosure
- Consent
- Directory Information

FERPA Foundations: Education Record

- Directly related to specific student
- Maintained by education agency (or agents)
- Any format
- Excludes “sole possession” notes, peer-graded papers
  - Some types of counseling notes *may* be “sole possession” notes

FERPA Foundations: Access & Disclosure

- Access: to actively view or retrieve information
- Disclose: to permit access to/release of information
- End Result: PII from education records is shared
- Authorized or Unauthorized
- “Legitimate educational interest”

FERPA Foundations:
Personally Identifiable Information

- Any information that can identify an individual
- Single details
- Combination of details
- “Regular” PII vs. Sensitive PII

FERPA Foundations: Consent

- Permission to disclose information
- Must be specific
- Must be written
- Generally required

FERPA Foundations: Directory Information

- PII from education records
- Not harmful, invasive if disclosed
- Partially defined by Student DATA Act* in WV
- Opt-out is possible

* Student Data Accessibility, Transparency, and Accountability Act (Student DATA Act), W. Va. Code §18-2-5h

Advanced FERPA: Exceptions!

- Directory Information
- **School Officials**
- **Outsourced Services and Functions**
- Enrollment and Transfer
- Research Studies
- Audits and Evaluations
- **Health and Safety Emergencies**
- **Judicial Order/Subpoena**
- Parents of 18 year-olds*
- …and more!

Talk it out!

What would you do if this happened to you?

Scenario: Peer Sharing with a Colleague

Mrs. Campbell is concerned about Brent. He's struggling emotionally and academically in her class. She wants to talk with the counselor to find the best way to support Brent and help him be successful.

Will FERPA let the teacher and counselor talk about Brent's situation and performance?

What limits might there be?

Scenario: Peer Sharing with a Colleague

Will FERPA let the teacher and counselor talk?

Yes! Both have a legitimate educational interest!

What limits might there be?

Use a private setting (no hallway chatter). Don’t involve others unless they have a legitimate need.

Scenario: Public Parent Discussions

Sally sees Ms. Perry at the local Wal-Mart. She has wanted to talk with someone at the school about her daughter. Susie has been getting sent to the office a lot and has been failing in math. Sally approaches Ms. Perry in the produce aisle and starts to ask about Susie's grades and discipline issues.

What should Ms. Perry do in this situation?

Scenario: Public Parent Discussions

What should Ms. Perry do in this situation?

Run! (Not really…)

Ms. Perry should do her best to decline to talk about it in the produce aisle (or other public spaces). Ask Sally come to the school for a meeting with the teacher or principal or set up a call later to discuss.

Scenario: Dealing with Threats

Leonard made some concerning posts on Instagram that police are saying constitute threats to his classmates and teachers. Police officers are at the school asking for Leonard's class schedule and other information—including counseling notes.

What should the school do in this situation?

Scenario: Dealing with Threats

What should the school do in this situation?

Cooperate with the police. Provide necessary information.

FERPA permits the sharing of information during health and safety emergencies to keep students, staff, and the community safe.

Caring While Sharing

Different rules apply to different contexts. Educators must apply critical thinking before sharing information.

Before Sharing, Ask Yourself…

- **Who**___am I sharing with?
- **What**__am I sharing?
- **Why**___does this person want/need it?
- **When**__can I share this information?
- **Where**_am I going to share it?
- **How**___am I sharing the information?

Consequences of Breaching Confidentiality

- Loss of federal funds
- Potential criminal and civil liability
- Loss of access
- Loss of license
- Potential harm to students!

Talk it out!

What would you do if this happened to you?

Scenario: Requests from Police/Law Enforcement

Officer Jackson has come to the school requesting information about Timmy's attendance and discipline issues. He's in a little trouble for something he did last weekend, and the Officer wants some additional information about what's going on with him.

Does FERPA permit the officer to have access to student records? What limits might there be?

Scenario: Requests from Police/Law Enforcement

Does FERPA permit the officer to have access to student records?

Maybe, but probably not.

What limits might there be?

Officer Jackson needs to produce a subpoena or court order, and Timmy's parents need to be notified first.

Scenario: Requests from Child Protective Services

Nancy, a case worker with DHHR, comes to the office requesting information about two sisters. Their parents are under investigation for neglecting and abusing the girls, and the case worker is gathering information about the girls' welfare.

Does FERPA permit the sharing of information with child welfare workers? What limits might there be?

Scenario: Requests from Child Protective Services

Does FERPA permit the sharing of information with child welfare workers?

Yes, absolutely!

What limits might there be?

Share the minimum needed unless/until the worker provides verification that the child is in state custody.

Scenario: Subpoenas and Court Orders

Prosecuting Attorney Casto has come to the school with a subpoena for information from 17-year-old Jackie's education and counseling records. The information will be used to prosecute Jackie for a disciplinary offense that rose to the level of a crime.

What should the school do in this situation?

Scenario: Subpoenas and Court Orders

What should the school do in this situation?

Schools must comply with lawfully-issued subpoenas. However, the school must *first* make a reasonable attempt to notify the child's parents (or the student, if he/she is 18 or older) about the subpoena. The notification is to give parents (or eligible students) the opportunity to have the subpoena quashed.

Staying in Control

Educators enact privacy protections in a number of ways—in the classroom and beyond.

Physical Controls

- Locking drawers, cabinets, etc.
- Clear workspace
- Screen protectors
- Safe file transport
- Smart use

Technical Controls

- Secure systems and devices
- Safe/secure storage
- User authentication
- Strong passwords
- Threat scans
- Smart use

Personal Controls

- Awareness
- Training
- Caution
- Notification
- Discretion
- Smart Use

Data Access

- Secure
- Limited
- Role-based
- Official duties only

Bonus! You can learn more!

- NCES Forum Guide to Education Data Privacy
  https://nces.ed.gov/forum/pub_2016096.asp
- USED Privacy Technical Assistance Center (PTAC) Online FERPA Training & Guidance
  https://studentprivacy.ed.gov/training
  https://studentprivacy.ed.gov/content/online-training-modules
- WVDE Support & Compliance Team!

Bonus! You can learn more!

- ASCA Standards
  https://www.schoolcounselor.org/school-counselors/standards
- ASCA Legal & Ethical Resources Page
  https://www.schoolcounselor.org/school-counselors-members/legal-ethical
- ASCA FAQs
  https://www.schoolcounselor.org/school-counselors-members/faqs

Bonus Tip! Caveat Emptor…

Products developed for school and classroom use often boast about being “FERPA Compliant.” Let’s explore that phrase…

My filing cabinets are FERPA Compliant!

But are they <u>really</u> FERPA Compliant?

No! No! Maybe? It depends…

When you hear "FERPA Compliant," remember

- Compliance **is not about tools**.
- Compliance is about actions.
- Compliance is about critical thinking.
- Compliance **is about people**.

Practical Privacy Protections

Tips for keeping your kids and colleagues safe.

Know what you need and why you need it.

Make sure you understand what data you need to use and why you need to use it. Don’t access or use data for any other purposes.

Protect your neighbors' privacy.

Recognize that you may have access to information about students and teachers in your communities that is private or sensitive. Treat all information with care!

Share with care.

Before you provide any information, make sure that you are providing only what's required and that you are using the most appropriate option for sharing.

Information Sharing Options

Secure Cloud Solutions

Direct system access

Shared network folders

Secure FTP

Not Options

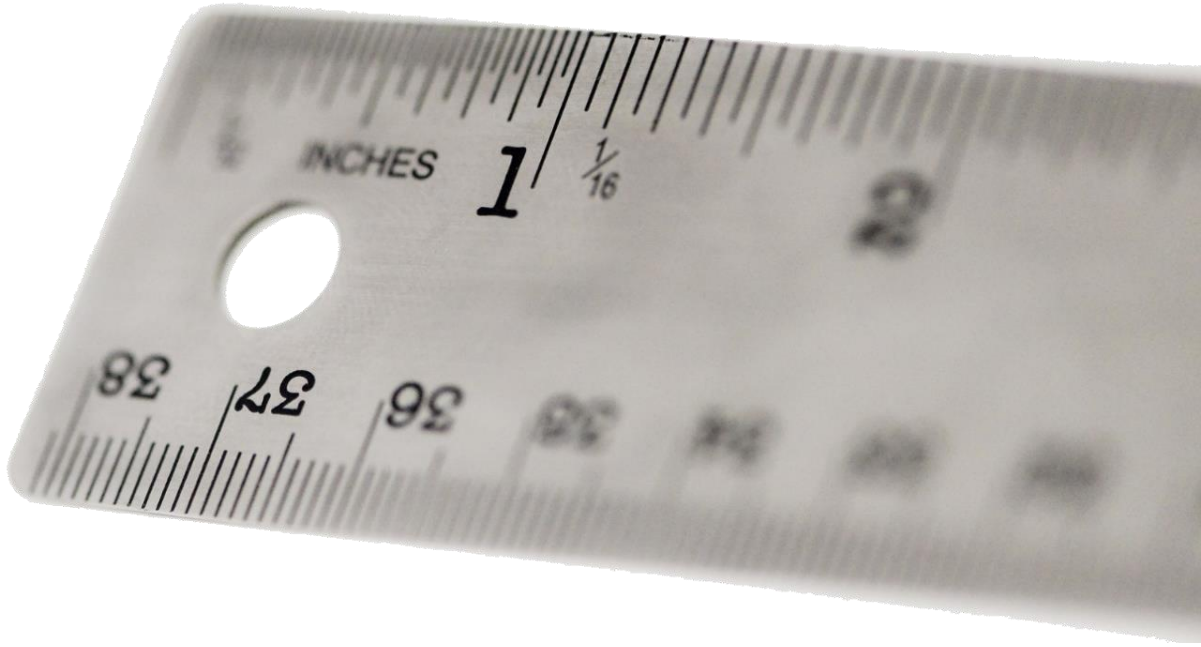
Removable/losable media

Email*

Insecure Cloud Solutions

Do as little as possible when sending data.

Data minimization is crucial for protecting privacy. If you must send information about individuals, use **only** the student ID numbers (not names) and the minimum amount of information necessary.



Trust, but verify.

Auto-complete is terrific—and also a terrific risk. Double- (and triple-) check to ensure that your email is going to the person you really want it to go to.

Act like your emails are public documents.

In fact, @K12 or other district emails may be subject to FOIA requests. Do all you can not to send PII about students, colleagues, or others via email. If you must, treat it as if you were sending your own information.

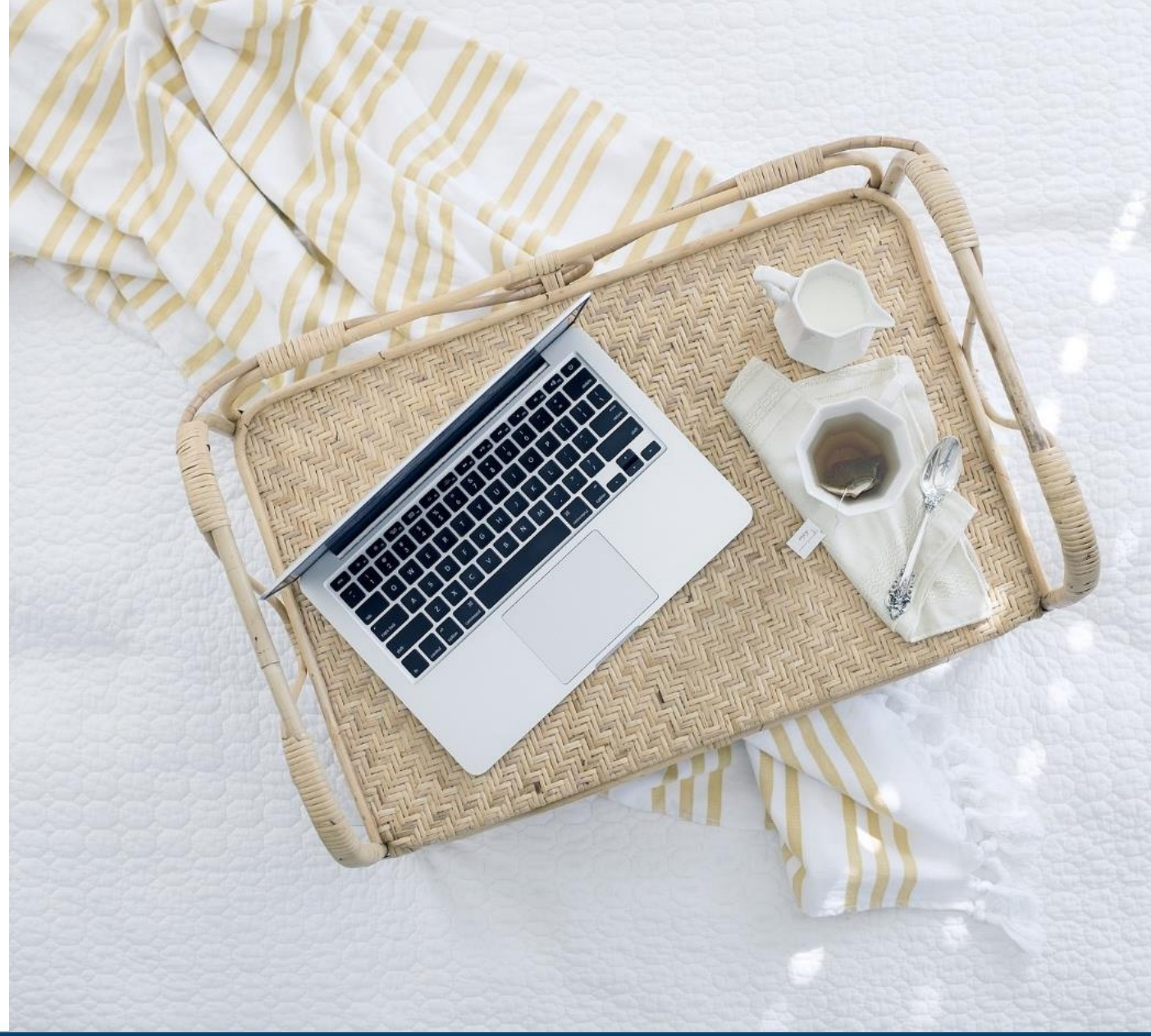
Documents subject to a FOIA request can be redacted to remove PII, but try to do all you can to save time and effort for legal and administrative staff who do the redaction!

FOIA is about your work, not about your devices.

Any state or district business conducted on personal devices is still subject to FOIA.

Relax! Don’t do it!

Do not open or store sensitive information on personal devices. Doing so constitutes a security breach. (Besides, when you’re on your own time, you should be relaxing!)



Keep it secret!
Keep it safe!

Do all you can to ensure that other people—coworkers, family members, complete strangers—cannot see or gain access to private or confidential information.

Just say, “No!”

Do not store passwords in your Internet browser or other applications. Storing your password is just like not having one to begin with!

Log out and lock it down.

Make sure to log out of all applications that may include private or confidential information. Close browser or explorer windows, just to be safe. Lock your other devices and filing cabinets when not in use.

Papers are data, too.

Data includes not only information stored in the student information system or other electronic sources. Profiles, reports, applications, and other paper-based records are also rightfully considered data and should be treated as such.

Watch your mouth.

"Loose lips sink ships." Make sure you use your best judgement and discretion when you must talk about sensitive information with colleagues. Try to avoid talking about sensitive topics or information in public settings.

Data Walls can be dangerous.

Data walls can be helpful or harmful. It all depends on how they're done.

Aggregate data is great!

Individual student data* should not be displayed in classrooms.

Virtual options may be better!

Keep your eyes on the horizon…

Guarding students' privacy is a crucial part of educators' every day jobs. Always be on the look-out for possible threats—and ways to improve!