****

**Facilitator Guide – Student Data Privacy Check-Up**

**What is in this Guide?**

This guide provides facilitators with the information they need to conduct a workshop around the essential components of state and/or district digital learning plans. It is our assumption that the facilitator will have at least a basic knowledge about learning in the digital age. Ideally, the facilitator should understand the basic components of a digital learning plan.

This guide provides facilitators with step by step activities, with suggested times for each activity, as well as narrative content and resources to support the topic. This guide is accompanied by a presentation slide deck for use during the workshop. It also includes a link to the logistics spreadsheet to help facilitators plan the workshop. Logistics include recommendations for audio visual, catering, registration and outreach.

This facilitator guide can be used in its current format or it is easily customizable to meet your needs. The guide is organized as follows:

* Purpose of the workshop
* Objectives for participants
* Key sections with suggested times
* Resources

**Purpose**

The goal of this session is to provide school and district leaders with the opportunity to check in and discuss current student data privacy practices, and to identify areas for improvement.

**Objectives**

* Learn more about data privacy
* Collaborate with colleagues to learn the current status of privacy programs
* Assess the strengths and challenges of your school’s privacy program
* Explore ways to engage parents
* Acquire resources supporting student data privacy
* Develop and maintain relationships with other district and state leaders

**Session Overview (90 minutes)**

* Welcome and Introductions (5-10 minutes)
* Background (10 minutes)
* Exemplar Rapid Fire Presentations (10-15 minutes)
* Policies (5-10 minutes)
* Establishing a Student Data Privacy Program (10-15 minutes)
* Strengths and Challenges (10-15 minutes)
* Parent Engagement (5-10 minutes)
* Reflection and Wrap Up (5-10 minutes)

\*\*Please note – the timing of activities requires a rapid paced session. Each facilitator will need to consider their audience (as related both to background knowledge and size) as well as future opportunities for professional learning opportunities around the topic and then choose the activities and time commitment for each.

****

**Welcome and Introductions (5-10 minutes)**

***Facilitator Note:*** *Introduce yourself, review the agenda and logistics for the session. Introduce the welcome activity. This activity will help the facilitator better understand the audience. If you have a large group, ask the participants to complete this via individual tables vs whole group. You can also choose an activity from the Activity Toolbox.*

**Personal Data Inventory**

Share your name, title, school or district and how many different online accounts you personally have for the following:

* Social Media
* Personal Finances
* Work Place
* Email

Ask the participants to total up the number of different accounts they have in their personal capacity for various online properties. Next, ask participants to stand up and move into number order based on the total number of usernames and passwords. Lastly, reflect on the vast number of online accounts and all of the different companies that maintain data sets on the individuals in the room*.*

**Background (10 minutes)**

***Facilitator Note:*** *This activity discusses the importance of student data and*

*highlights the Privacy Technical Assistance Center (PTAC) as a “one-stop” resource.*

**Overview**

The [National Education Technolopy Plan](https://tech.ed.gov/netp/) discusses how the use of student data is crucial for personalized learning and continuous improvement (see [Section 4: Assessment](https://tech.ed.gov/netp/assessment/)). Acting as the stewards of student data presents educators with several responsibilities. School officials, families, and software developers have to be mindful of how data privacy, confidentiality, and security practices affect students. Schools and other educational institutions should be certain that policies are in place regarding who has access to student data and that students and families understand their rights and responsibilities concerning data collection. Districts should have a policy or procedure for reviewing third party agreements in the terms of service or contract for compliance around use, protection (data security) and destruction of student personally identifiable data.

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a “one-stop” resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. Anyone can contact PTAC for information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems.

***Facilitator Note:*** *Choose the featured video. This activity will help participants learn more about privacy issues when using technology. It also provides an opportunity for dialogue and to share experiences. Choose whole group, table or partner discussion depending on timing and size of group*

[PTAC’s Protecting Student Privacy Training Video](http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services-training-video)

This video offers a short summary of student privacy issues while using technology and provides some examples to help educators identify which online educational services and applications are privacy-friendly.

**Discussion Questions**

* What does transparency mean to you, with regard to educational technology, privacy, and parents?
* How transparent is your district with regard to student data collected by the school or third parties (e.g., online educational service providers)?

****

**Exemplar Rapid Fire Presentations (10-15 minutes)**

***Facilitator Note:*** *Ask one or two exemplar school/districts to share an example of a FERPA annual notice from the LEA. The presentations should be 5-7 minutes and prepared in advance of the workshop. Additional information about presentations can be found in the Logistics resource.*

**Discussion Questions:**

* How is your school/district similar to the exemplar?
* Are there policies/practices shared that your school/district can implement within the next quarter?

**Policies (5-10 minutes)**

***Facilitator Note:*** *Share the notes below about privacy laws. This will provide the participants with additional background knowledge.*

Federal and state privacy laws are likely to impact the collection and use of student data.

The [Family Educational Rights and Privacy Act](http://familypolicy.ed.gov/ferpa-school-officials) (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that affords parents the right to inspect and review their children’s education records, the right to seek to have the education records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 or enters a post-secondary education institution at any age, the rights under FERPA transfer to the student. Students to whom FERPA rights have transferred are termed eligible students.

FERPA generally requires that parents or eligible students provide prior written consent before schools can share personally identifiable information from a student’s education records, unless an exception applies. For example, when schools and districts use online educational services, they must ensure that FERPA requirements are met. Typically, the FERPA school official exception to consent will apply to schools’ and districts’ use of online educational services. The U.S. Department of Education issued best practice guidance to address questions related to student privacy and the use of online educational technology in the classroom, available at <http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services>.

[The Protection of Pupil Rights Amendment](http://familypolicy.ed.gov/ppra) (PPRA) (20 U.S.C. § 1232h; 34 CFR Part 98) governs the administration to students of a survey, analysis, or evaluation that reveals information concerning one or more of eight protected areas, including, but not limited to, sexual behaviors and attitudes and illegal, anti-social, self-incriminating, and demeaning behavior. PPRA also concerns marketing surveys and other areas of student privacy, parental access to information, and the administration of certain physical examinations to minors.

The [Children’s Online Privacy Protection Act (COPPA)](https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions) (15 U.S.C. § 6501–6505) governs online collection of personal information from children under age 13. For example, before a developer can collect any information from a student under 13, verifiable parental consent is required. The FCC, which enforces COPPA, has said that school officials can act in the capacity of a parent to provide consent to sign students up for online educational programs at school. The general guidance is that software companies are allowed to track students within their program, but COPPA prevents them from tracking those students across the Internet.

The [Children’s Internet Protection Act (CIPA)](https://www.fcc.gov/guides/childrens-internet-protection-act) (47 U.S.C. § 254) imposes several requirements on schools or libraries that receive E-rate discounts for Internet access. Schools and libraries must certify that they have an Internet safety policy that includes technology protection measures. These protection measures must block or filter Internet access to pictures that are obscene, pornographic, or harmful to minors, and schools also must monitor the online activities of minors. Because most schools receive E-rate funds, they are required to educate their students about appropriate online behavior, including on social networking websites and in chat rooms, and to build cyberbullying awareness. Particularly if a digital learning resource requires networking among students, schools must comply with CIPA.

[IDEA](http://idea.ed.gov/) also provides confidentiality protections and often additionally will protect information for students with disabilities.

**State Laws**

Many states have passed student data privacy legislation in the past few years. Review your state laws for updates and additional laws on student data privacy. For the most recent privacy laws and bills in your state, the National Conference of State Legislatures has up to date information available to assist you in determining the relevant privacy laws: <http://www.ncsl.org/research/education/student-data-privacy.aspx>

****

**Developing a Privacy Program (10-15 minutes)**

***Facilitator Note****: Share the featured video. Choose whole group, table or partner discussion depending on timing and size of group*

**PTAC’s Developing a Privacy Program**

The video addresses the legal and ethical requirements for student data privacy. It also discusses transparency requirements.

<https://youtu.be/clcJ_6n2qPA>

**Discussion Questions**

* What do you know about your school’s privacy program?
* Do you know what your state student privacy statute requires?
* Do your students and families understand their rights and responsibilities concerning data collection?
* How are you protecting your students and families?
* Does your district have policies or procedures in place for reviewing third party agreements for compliance around use, protection (data security) and destruction of student personally identifiable data?

**Strengths and Challenges Activity (10-15 minutes)**

***Facilitator Note:*** *Either via poster paper and markers or online collaboration tools have the participants brainstorm ways to improve their privacy policies and procedures, including communication with teachers, students and parents.*

**Discussion Questions**

* How is your school/district incorporating educational technology into the privacy program?
* What are your greatest strengths in protecting student privacy when using educational technology?
* What are areas of growth?
* How do you inform staff about changes in privacy policies?
* Do you offer annual training for new staff? If not, how would you go about setting one up?
* How is privacy information communicated to students?

**Parent Engagement (5-10 minutes)**

***Facilitator Note:*** *Share this video and encourage participants to think about how to share policies around student data privacy with parents. Share more details about how to effectively communicate to parents.*

[PTAC’s What Parents Need to Know about Their Student’s Data](https://youtu.be/Xa0cSA57fIQ)

<https://youtu.be/Xa0cSA57fIQ>

**Discussion Questions**

* How are parents involved in your school or district’s privacy program?
* How are parents informed about technology that collects data about their children?
* How can you improve communication with parents about student data?

****

**Reflection and Wrap Up (5 minutes)**

***Facilitator Note:*** *Take a few moments to reflect on the session, share details about additional events related to the remainder of the day and engage the audience to take action when they return to their schools/districts. Use this activity or choose another one from the Activity Toolbox.*

**Two Stars and a Wish Activity**

* Share two things your school/district is doing well related to student data privacy.
* Share one thing you plan to work on based on your return to the office.

Based on the reflection activity, identify the next steps for your state, district or school.

**Wrap-Up**

***Facilitator Note:*** *The facilitator wraps up the day and shares resources with participants. Sample language: “This is only the first step of many steps in supporting teachers and students for learning in the digital age. I encourage you to follow up on our reflection activity during the next few weeks and continue to collaborate with your peers. Think about what tools and resources you can use to maintain relationships and encourage collaboration, as well as identify opportunities for on-going professional learning and workshops.*

**Resources**

The US Department of Education does not endorse any resources; instead they are provided to assist the facilitator in preparing for the workshop. The facilitator can also share these resources with participants to support on-going professional learning and school/district planning after the workshop. For example, some districts have used the NETP for on-going book studies throughout the school year to support the development and refinement of technology initiatives.

**US Department of Education Resources**

[Checklist for Developing School District Privacy Programs](http://ptac.ed.gov/document/checklist-developing-school-district-privacy-programs-august-2015).

[National Education Technology Plan](https://tech.ed.gov/netp/)
[Policies for Users of Student Data: A Checklist](http://ptac.ed.gov/sites/default/files/Policies%20for%20Users%20of%20Student%20Data%20Checklist.pdf)

Privacy Technical Assistance Center

[Privacy Technical Assistance Center Videos](http://ptac.ed.gov/ptac-guidance-videos)

[Protecting Student Privacy while Using Online Educational Services: Requirements and Best Practices](http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29.pdf)

[Protecting Student Privacy while Using Online Educational Services: Model Terms of Service](http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf)

**Facilitator Guide Resources**

[California Student Privacy Alliance](http://cetpa.net/CETPA/Programs/Student_Data_Privacy/CETPA/Programs/Student_Data_privacy.aspx?hkey=273f444c-8f38-4b41-a95a-4e214d940029)

[Common Sense Media’s District Privacy Evaluation Initiative](https://www.commonsense.org/education/privacy/about/main)

[Consortium for School Networking (CoSN) Trusted Learning Environment](http://trustedlearning.org/about-the-seal/)

[Data Quality Campaign’s State Legislation Overview](https://dataqualitycampaign.org/resource/2016-student-data-privacy-legislation/)

[Future of Privacy Forum’s FERPA SHERPA](https://ferpasherpa.org/)

[iKeepSafe’s FERPA assessment](http://ikeepsafe.org/privacy/ferpa/)

[Massachusetts Student Privacy Alliance](https://secure2.cpsd.us/mspa/about_mspa.php)

[Student Privacy Pledge](https://studentprivacypledge.org/)