PTAC Toolkit for LEAs:

Staff Policies and Teacher Access

March 24, 2014

Baron Rodriguez, PTAC Director
Mike Tassey, PTAC Security Consultant

Today's Presentation

- Toolkit for the school districts – overview
- Privacy & security best practices
  - General policy considerations
    - Data governance
  - Specific recommendations
    - Data access and use
    - Data destruction
    - Transparency
- Wrap up and Q&A

PTAC Toolkit for LEAs

Overview

Toolkit for the School Districts

- Best practice guidance & training materials for LEA staff
  - Online educational services & protecting student privacy
    - Vendor contracting
    - Access use policies
  - Data destruction
  - Transparency
- User-friendly format
  - Videos
  - Checklists & single-page summaries

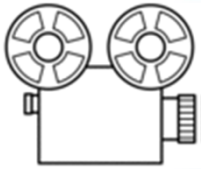


Photo courtesy of hywards / FreeDigitalPhotos.net

LEA Toolkit Materials – Available Now

- **NEW!** Protecting Student Privacy While Using Online Educational Services
  - This guidance clarifies questions related to student privacy and the use of educational technology in the classroom: http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services

Photo courtesy of Stuart Miles / FreeDigitalPhotos.net

Upcoming LEA Toolkit Materials

- Data privacy
  - *FERPA Exceptions* "cheat sheet"
  - *Online Educational Services—Vendor Contracting Provisions* checklist
  - *Protecting Student Privacy While Using Online Educational Services* video for LEAs & school staff
- Data security
  - *Best Practices for Data Destruction* brief
- Transparency
  - *Transparency Best Practices Regarding Data Privacy for Schools and Districts* brief

General Policy Considerations

Data Governance

Policy & Data Governance

- Establish a comprehensive data governance plan
  - Specify data security & privacy policies and procedures
- Conduct an inventory of sensitive data
  - Know what data you collect, what it's used for, and how it's protected
- Conduct an inventory of all assets used in your computing environment (e.g., physical devices, applications, and online educational services)
  - Organization- and user-managed devices (e.g., tablets)
  - Free, paid, and "freemium" apps and services

Photo courtesy of Stuart Miles / FreeDigitalPhotos.net

Policy & Data Governance

- Conduct staff training and provide professional development resources
  - Train staff about data security, including best practices for emailing confidential data
- Periodically audit staff activities for compliance
- Create procedures and environment where staff can report policy violations and security incidents promptly and without fear of retribution
  - Establish a single point of contact at the LEA whom schools can easily access for legal & technical assistance

Data Access & Use – Policy & Controls

Best Practices

Access & Use Policy

- For each user category (e.g., administrators, teachers, volunteers, etc.), list and clearly spell out data uses and activities that are allowed and prohibited
  - Supplement the list with specific examples
  - Include requirements for employing “Click-Wrap” consumer apps
    - Specify who has authority to accept the Terms of Service

- Clarify under what circumstances an exception may be granted to lift the restrictions and how long the exception would apply

Photo courtesy of Stuart Miles / FreeDigitalPhotos.net

Role-Based Access Control

- Define roles and privileges for users
- Limit administrative privileges to minimize the risk of unauthorized disclosure
- Restrict physical access to sensitive data and resources
  - Limit access to approved individuals who require access to perform work duties
    - Example: A school district may restrict access to student-level data to only those staff who are directly involved in managing data collection from schools or entering data into an SLDS

Access Control – Implementation

- Maintain tight control of available ports, protocols and services to reduce vulnerability to attack and misuse of data systems
  - Implement a change control policy to track which ports, protocols, and services are allowed internally and through the system boundary
- Review and update access controls regularly
  - Evaluate data systems and security controls every 1-3 yrs. or when a system or environment changes significantly
    - Changes in data system, staff duties, privacy laws, technology, etc.

Access Control – Enforcement

- Ask staff to sign a statement of assurance as a condition for accessing sensitive student data
- Periodically audit staff activities for compliance
  - Check for adequate password protection and compliance with data access restrictions
- Check the system for unauthorized or unwanted data access
  - Monitor attempts to access restricted use data by unauthorized staff
  - Revoke access by individuals who are no longer employed or staff whose duties no longer necessitate student data access

Staff Access Control Policies – Q&A

- Is it a best practice to include data confidentiality in job descriptions?
- *Confidentiality Policy* - what would be a good statement of confidentiality that districts can ask staff to sign?
- What are some best practices around *Technology Use Policy*?
- What *Disciplinary Policy* do you recommend if there is a disclosure?
- What other policies do you recommend putting in place to ensure timely and efficient response to a disclosure?

Data Destruction

FERPA Requirements &

Best Practices

FERPA Requirements

- FERPA generally requires that PII from education records disclosed to an outside party under either the "studies" or the "audit/evaluation" exception to consent are destroyed by the outside party when no longer needed for the purposes for which it was originally disclosed (34 CFR §§ 99.31(a)(3) and (a)(6) and 99.35)
- FERPA does not require destruction of education records maintained as a part of the regular school or agency operations
  - Many jurisdictions require lengthy retention periods for student attendance and graduation information

Photo courtesy of suphakit73/ FreeDigitalPhotos.net

Best Practices – Within the Organization

- Formalize and document data destruction processes
  - Address both electronic and non-electronic records (e.g., paper)
  - Require partner organizations to adopt the same policies
- Use appropriate data deletion methods to ensure the data cannot be recovered
  - Talk to your IT professional to ensure proper deletion of records
    - See NIST's Guidelines for Media Sanitation for technology best practice standards

Best Practices – Data Shared with Third Parties

- In written agreements, specify that the third party must destroy all provided PII when no longer needed for the purpose for which it was provided
  - Include copies of the PII (e.g., system backups, temporary files, or other storage media)
  - Specify the type of destruction to be carried out
- Ensure accountability for destruction
  - Ask the individual responsible for performing the destruction to sign the certification form which describes the details of the destruction

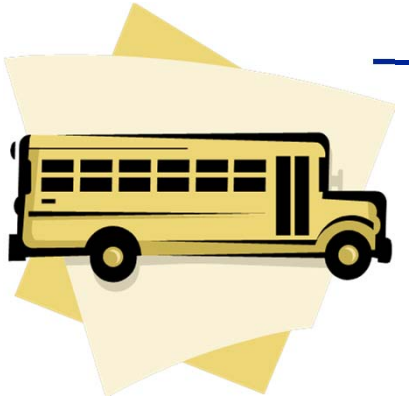
Photo courtesy of patrisyu/ FreeDigitalPhotos.net

Transparency

Best Practices

Communication of Data Privacy Policies & Practices

- Clearly communicate with parents and the public on how students' privacy is being secured
  - Use your website to post information about data privacy policies and practices
- Describe in detail what education data your district collects and how it maintains, uses, and/or shares the data with other entities
  - Include data breach policies and other useful information about your data security efforts, including how you protect any data that may be stored in the cloud
    - Be specific and use plain language
    - Provide examples whenever possible



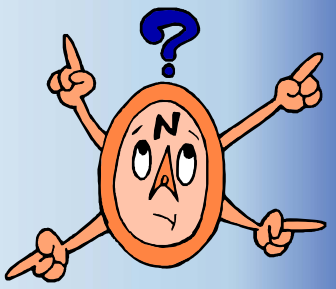
Inquiries About Data Privacy

- Keep the lines of communication open
- Review parental inquiries, concerns, and suggestions in a thoughtful and careful manner
- Respond to parental inquiries in a timely manner
- Periodically review old inquiries and resolutions to evaluate and improve your communication and transparency efforts
- Review and modify privacy policies and procedures, including the content of privacy notices and modes of communication, at least annually

PTAC Resources

- PTAC - New Guidance: Disclosure Avoidance & Limiting Access to PII (Dec 2012)
- Data Security Threats: Education Systems in the Crosshairs (May 2012)
- Case Study #1: High School Feedback Report (Jan 2012)
- Checklist: Data Security (Dec 2011)
- Issue Brief: Data Security: Top Threats to Data Protection (Dec 2011)
- Issue Brief: Data Security and Management Training: Best Practice Considerations (Dec 2011)
- More at **http://ptac.ed.gov/**
  - Data security, privacy, disclosure avoidance, data governance, data sharing, legal references, FAQ, video trainings, webinars, and other events!

Wrap Up and Q&A Time



- Teacher Access to SLDS or other data systems – What are some best practices in terms of data teacher should or shouldn't be able to see?
- What circumstances should districts be aware of when it comes to sharing student data between staff?
  - Ex: Can a teacher see the health records for his/her student?
  - Ex: Can a teacher see the grades or state test results for his/her last year students?
  - Ex: Can student PII (e.g., names) be shared with Professional Learning Communities (PLCs) that are looking at student performance?
- Other questions or feedback?

Contact Information

Privacy Technical Assistance Center

Telephone:	(855) 249-3072
Email:	privacyTA@ed.gov
FAX:	(855) 249-3073
Website:	http://ptac.ed.gov