Louisiana Believes

Building Strong Data Governance and Privacy Protocols

Data Governance and Privacy Plan Development

January/February 2017 Supervisor Collaborations

DEPARTMENT of EDUCATION

Outcomes

In this session, participants will

- Review areas where protections are needed.
- Discuss possible policies, processes, and practices to provide protections
- Review template and exemplar policies, processes and practices.
- Complete a "Strong Protocols" guide formalizing individual next steps that will result in implementation of strong protocols.

Developing a Data Governance and Privacy Plan

STEPS FOR ESTABLISHING A DATA GOVERNANCE AND PRIVACY ACTION PLAN

✓ **Step 1: Know the Laws**	Laws provide a baseline of protections for students and families.
✓ **Step 2: Build a Team**	Who should be on the data governance and privacy team? Who should be building privacy policies and practices?
✓ **Step 3: Provide Training**	Use education of all stakeholders as the foundation of your plan.
Step 4: Build Strong Protocols	Adopt norms and policies for all data and technology use and for managing contractors, apps, and devices. Implement workable processes.
Step 5: Make Security a Priority	Hold all data users and managers accountable. Ensure legally binding agreements to hold contractors accountable are established.
✓ **Step 6: Involve Parents**	The ability to communicate and build trust with parents is essential. Empower families to help take charge of their children's education.

Areas to Protect

Security	Privacy	Safety
Online Apps Usage	Non-disclosure Agreement	Filters
Access Control	AUPs	Privacy Controls to Limit Sharing
Password Management	Data Sharing Agreements/Contracts	AUPs
Locking Computers	Disclosure Avoidance Techniques	
Network Security		
Patch Management		

“Ask Before You App”

Online Services: Recognize the Risks

- “In 2016 an audit of some 1,200 Web-based education software products by the nonprofit Common Sense Education found that nearly half the offerings didn’t automatically encrypt student data.”
- “Even when an app has additional privacy settings, many teachers are either unaware of the options or don’t bother changing the defaults, according to Sophia Cope, a staff attorney for the Electronic Frontier Foundation, a watchdog for civil liberties in the digital world.”

—The Hechinger Report

Online Services:
Mitigate the Risk with Free Tools

- Student Privacy Pledge – Companies agreeing to protect student data
  - *Student Privacy Pledge Reaches Milestone of 300 Signatures*- Future of Privacy Forum
- Common Sense Education – Reviews and Ratings of Web Apps
- Houston Independent School District – Reviews of apps grouped by use

Online Services:
Mitigate the Risk with Policy and Process

- Ouachita's Policy and Process
- St Tammany's Policy and Process
- Ascension's Policy and Process
- Teacher Led Model
  - Survey

Tools for Processing MOUs and releasing data:

- MOU Routing Template
- Data Release Checklist
- Software tracker – Ascension Parish School Board
- Contract Information Form – Ouachita Parish School Board
- Website Application for Approval – St. Tammany Parish School Board

Contracts and Agreements

Contracts, agreements, or memorandums of understanding (MOUs) are required by FERPA and R.S. 17:3914 to ensure security of student data.

Necessary Elements:

- What data will be collected (data)
- Why the data will be collected and how it will be used (purpose of disclosure)
- How the data will be protected (confidentiality ,restrictions on use)
- How security audits will occur (security audits)
- How security breaches and notification of security breaches will be addressed (security breach)

Sample Contract Language – St. Tammany Parish School Board

Turn and Talk

Discuss the following with your shoulder partner and be ready to report out to the group.

- What online services policies, processes, and tools does your LEA already use?
- What new tool would be the most helpful?

Acceptable Use Policies

Acceptable use policies establish how individuals (staff and students) should interact with technology and data. These policies should include:

- What is acceptable
- What is not acceptable
- Consequences

Often times nondisclosure agreements are used with staff.

Samples:

- Ascension Parish School Board
- NCES

Turn and Talk

Discuss the following with your shoulder partner and be ready to report out to the group.

- With which policies do you have the most difficulties getting staff to comply?
- What tools to support policies do you already use?
- What new tool would be the most helpful?

Data Releases and Disclosure Avoidance Techniques

When LEAs, schools or the LDOE release reports publicly, it is important to ensure that students cannot be identified. Aggregated data minimizes the risk of disclosure; however, some risk remains. Below are some considerations when releasing data.

Sensitive PII is PII that if accessed or released the individual could experience an adverse impact (e.g., social security number, name and mother's maiden name).

The risk of re-identification must be considered. It's unlikely that a student's identity could be derived from a state level report on the counts of students expelled; however, if the report contains the LEA, the school, and the grade level the risk that the student might be identified a member of the community increases.

Turn and Talk

Discuss the following with your shoulder partner and be ready to report out to the group.

- Does your LEA publish or release data about students?
- If so, does your LEA employ disclosure avoidance techniques?
- If so, what techniques do you use?

Next Steps

- Review the “Strong Protocols Chart” completed during presentation and determine what changes are needed for your LEA
- Complete the Data Governance Planning Survey

Questions?

Kim Nesmith, M.Ed.
Data Governance and Privacy Director
Kim.Nesmith@la.gov