LEADING EDUCATION INNOVATION

PROTECTING PRIVACY IN CONNECTED LEARNING INITIATIVE

Trusted Learning From the Ground Up: Fundamental Data Governance Policies and Procedures

NOVEMBER 2019

As school systems build and grow their data protection programs, they need to craft a solid foundation of documented privacy Policies and Procedures to guide and govern employee behavior. Understanding the differences between them, and the policies and procedures that should be part of the foundation of school system data governance work, is the first step in creating comprehensive and actionable documentation for your data protection program.

What is the difference between a policy and a procedure?

Policies and procedures are not interchangeable. Policies set the tone and articulate the high-level requirements, while procedures give action to policies.

- Policy *(why we do it)* – A policy is a set of guiding principles or rules intended to influence decisions and actions.
- Procedure *(what we do and how we do it)* – A procedure describes the actions an organization performs in order to achieve the policy result. Organizations may use various terms to further define this function.

Policies vs. Laws

Some policies address the district's commitment to abide by a given federal or state law. These should not restate the law, but rather articulate the district's compliance requirements. Each such policy should be accompanied by procedures that detail how the district will abide by those requirements. For example, FERPA has a number of annual requirements including that schools must notify parents of their rights under FERPA, describe how they define a school official, explain what data they consider to be directory information and how parents may exercise their rights under FERPA[1]. While there may be a policy in place articulating the school system's commitment to comply with these requirements under FERPA, each of the specific requirements needs an accompanying procedure to detail what employees are to do in order to ensure that the school system executes on each of those requirements. In addition to FERPA, there are other applicable federal laws as well as more than 125 state student data privacy laws.[2]

Policies vs. Standards

Standards are formally established, quantifiable requirements that apply to processes, actions, and configurations. A standard can be internal to the organization or external, such as an industry, association, national, or international standard (e.g. NIST, ISO).

1 For more detailed information on Federal privacy laws, download CoSN's Protecting Privacy in Connected Learning Toolkit
2 See https://ferpasherpa.org/state-laws/

District Policy and Procedures Checklist

The following checklist may serve as a guide for your school system for building and improving your data privacy and security program. Not all school systems may have all of these policies and procedures in place, but this checklist will help you measure your progress towards creating a holistic, documented data governance program.

How to Use this Document

This checklist provides school systems with the opportunity to inventory their existing data protection policies and identify any gaps. This exercise is one of the tasks that can be done to prepare to apply for the Trusted Learning Environment Seal. An editable version of this document is provided here as a spreadsheet.

	Foundation Policy List Information			Notes and Resources
	List of your District's regulations/policies related to privacy, security and digital safety (with date of last update)			These items provide the foundation for your future progress related to establishing and maintaining up to date, comprehensive governance policies and procedures.
	List of your District's procedures related to privacy, security and digital safety (with date of last update)			
	List of your state laws related to privacy, security and digital safety [1]			
	Policies		Procedures	Notes and Resources
Student Data: Family Educational Rights and Privacy Act				
	Annual Notice of Rights that includes:		We have a procedure in place that details who is responsible for updating the notice annually as needed, sending it, tracking responses and conducting any necessary followup.	• The U.S Department of Education's Privacy Technical Assistance Center ("PTAC") provides a Model Annual Notification that addresses many of the elements listed at left.
	Definition of School Official			• In addition to a definition, school systems should provide clarity on who within the district has the ability to designate a third party as a school official.[2] • Many school systems already have clear policies on who is authorized to sign a contract on behalf of the district and may benefit from having consistent policies for this for both free and pain services. • Model Annual Notification (PTAC)
	Definition of Directory Information and Opt-Out process			• See the CoSN Privacy Toolkit for guidance on the use of a limited directory information policy. • Be aware of the requirements surrounding the use of student ID as an electronic identifier (username). • Note that some states have additional requirements related to the release of directory information. *Examples* • Baltimore County Public Schools (MD)
	Definition of Student Education Records			State laws may have additional applicable definitions.

1 The Future of Privacy forum maintains a list of state student privacy laws. There are also a number of organizations that track state Education legislation. For example, in Virginia, the Virginia Association of Secondary School Principals track bills in progress as does the Virginia Department of Education.

2 The US Department of Education has stated that "Schools and districts should be clear with both teachers and administrators about how proposed online educational services can be approved, and who has the authority to enter into agreements with providers"

	Parental request to inspect/amend/correct errors in the education record and request a hearing		Procedure for responding to parent requests to exercise their rights under FERPA or state law	• FERPA requires that schools fulfill a parent's request within 45 days. Some states impose a shorter time limit. • Parents whose children receive services under the Individuals with Disabilities Education Act (IDEA) may have additional rights regarding their child's education records.
	Release or posting of student work		Procedure and form for Media Release/Posting of Student Work	As with directory information, school systems should provide clear guidance to staff on the policies for posting student work, to district websites, media outlets and other third parties. *Examples* • Cambridge (1, 2)
	Disclosure to military recruiting officers/ opt-out		Military recruiting officers/opt-out process/ form	Access to High School Students and Information on Students by Military Recruiters (PTAC)
	Requests for Directory Information		Procedures for responding to requests for directory information	*Guidance* • Is opt out information stored in a location accessible to those responsible for fulfilling directory information requests and to teachers so they may refer to it prior to posting photos that include students?
	Student Information and Social Media		Procedure for any required approvals prior to posting, requirements to obtain parent approval and/or a checklist for ensuring the use case complies with policy and does not conflict with directory information restrictions.	*Examples* • Denver (1, 2) *Guidance* • Fairfax • Common Sense Media
Use of Student Data for Studies, Audit or Evaluation and other Research				
	FERPA Studies Exception Policy		Procedure for qualifying the recipient and approving data sharing. May include forms, contracts/data sharing MOUs, the method of securely transferring the data, and restrictions on use.	• FERPA Exceptions (Studies) Video • Model Written Agreement Checklist (PTAC) • Written Agreement Guidance(PTAC) • Case Study: High School Feedback Report (PTAC)
	FERPA Audit or Evaluation Exception (including establishing approval authority)		Procedure for qualifying the recipient and approving data sharing. May include forms, contracts/data sharing MOUs, the method of securely transferring the data, and restrictions on use.	• FERPA Exceptions (Audit or Evaluation) Video (Utah) • Model Written Checklist (PTAC) • Written Agreement Guidance (PTAC)
	Other Research not covered by FERPA Studies or Audit Exceptions (includes, but not limited to: *External academic researchers; journalists; teacher dissertations; articles or action research; vendor "white papers; nonprofits and advocacy groups*		Procedure for qualifying the recipient and approving data sharing. May include forms, contracts/data sharing MOUs, the method of securely transferring the data, and restrictions on use.	Policy should clearly define who has approval authority. *Examples* • Dysart Unified School District • Fairfax County Public Schools Policies and procedures may also be needed to provide guidance for staff members in the event that they would like to use data for research purposes that are external to their job (such as writing a thesis, dissertation, etc.), including the process for obtaining prior approval.

	Protection of Pupil Rights Amendment (PPRA)[1]		Procedures for reviewing student surveys, audits and evaluations to determine if PPRA applies; procedures for providing notice and handling opt/out.	*Policy* • PPRA Model General Notice of Rights (PTAC)
	Data Sharing with Community Organizations		Procedure for qualifying the recipient and approving data sharing. May include forms, contracts/data sharing MOUs, the method of securely transferring the data, and restrictions on use.	Many public and private nonprofit organizations, including community-based, professional, and faith-based organizations partner with schools and LEAs to administer vital academic, social, recreational, and vocational programs to students during the day, after school, and during the summer. • Guidance on Sharing Information with Community-Based Organizations (PTAC) Note that states may have additional laws related to school-affiliated entities.
	Technology Application Approval, Acquisition and Contracting Authority		Application Acquisition Approval Process[2]; Data Protection/Confidentiality Agreements	Strong policies and processes for the approval of applications that collect, store and use student data is a key component in maintaining direct control of a third party under the FERPA school official exception. In creating these policies and procedures, schools articulate who has the ability to designate a technology provider as a school official for purposes of sharing education records. School system policy should also clearly defines who has the authority to contract on behalf of the district for both free and paid services. The policy should address agreements that require a written signature and those that are binding via clicking online to agree. *Example Approval Process* • Raytown Quality Schools Data Governance Manual, Appendix C • Raytown Quality School, authorized signatures policy • Raytown Quality School, free resources • Denver Public Schools *Guidance* Data protection agreements (DPA) should be drafted and adopted by each district in coordination with their general counsel, and based on applicable federal and state laws and district policies. Districts may wish to consult the following resources when crafting or adopting a DPA. • CoSN Privacy Toolkit Suggested Contract Clauses • PTAC Model Terms of Service • Student Data Privacy Consortium

1 USED PPRA Model General Notice of Rights
2 Example P. 23, Raytown Public Schools Data Governance Manual and Fairfax County Public Schools

Training				
	Policy requiring periodic privacy and security training for staff with have access to education records		Process for maintaining record of training	*Example Training Policy* • Raytown Quality Schools, Security Awareness Program, Annual Security Training • Dysart Unified School District's student privacy training module is required as part of annual training. An internally developed system is connected to the courses in the LMS to track completion.
Security				
	Foundational Information			
	Require an internal and third party inventory of systems that collect and store student data		Checklist or related forms used in recording the inventory	CoSN Cybersecurity Resources • An Excel worksheet that can be used to inventory common system categories is available for downloaded from CoSN here. • CoSN Cybersecurity Self-Assessment • CoSN Cybersecurity Planning Rubric • CoSN Cybersecurity Planning Template
	Account Management & Access			
	Accounts and Passwords		Procedure and accompanying forms for provisioning, auditing accounts and revoking access	Account Request Procedure, Form • Baltimore County Public Schools *Guidance* • Note the special requirements for passwords when using student ID as an electronic identifier/username
	Account access for non-employee workers • Interns/Student Teachers • Volunteers and Contractors		Account Request Procedure and accompanying form for provisioning access, auditing and deprovisioning access.	School Volunteers and FERPA (PTAC)
	Systems Management			
	Audits		Procedure for conducting security audits, across systems, including schedules and risk-management frameworks to be used when addressing audit findings.	*Resources* • Responding to IT Security Audits (PTAC) *Guidance* • HIPAA (Bozeman) • PCI (Fairfax) • Email (Baltimore County Public Schools (MD) policy, process
Data Governance				
	Common components of a data governance policy include: • Policy and Procedure Oversight Responsibility • Data Stewards/Owners • Data Classification • Data Inventory • Data Storage			*Notes:* When developing your data governance policy, also consider specifying any unique requirements for both district and personal cloud computer storage, mobile device management and removable media that may be used in the school system, as well as implications of tools such as OneDrive, Google Backup and Sync, DropBox and related tools that sync local files to a cloud service.

Data Governance cont'd			

	• Data/Records
	• Data Archival and Backup
	• Data/Records Retention
			Examples of Data Governance from CoSN Trusted Learning Environment Recipient Districts:
			• Raytown Quality Schools (MO)
			• Baltimore County Public Schools (MD)
			• Park Hills School District (MO)
			• Howard County (MD)
			  • Governance
			  • Student Records
			
			Additional Resources:
			• Data Governance Checklist (PTAC)
			  • Data Destruction Best Practices (PTAC)
			  • Data Security for Schools, National School Boards Association
			  • University of Michigan

	Responsible/Acceptable Use		Procedure for ensuring distribution and tracking signatures	CoSN provides a guide for adapting AUPs in the age of mobile devices and social networks. While it is common to have separate AUPs for staff and students, also consider if additional language/versions are required for: Volunteers, Contractors, Interns/Student Teachers, SROs *Examples* Baltimore County Public Schools: Student policy, Staff policy For issues related to SROs, see School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (PTAC)
	Disposition/Destruction of Data and Devices Policy		• Records Retention Schedules • Audit Form • Data Disposition Guidelines • Device Trade-up Guidelines • Media Disposal Form	*Guidance* • Best Practices for Data Destruction (PTAC)
	Security Standards		Procedure for assessing and updating the standard as needed.	• NIST standard SP 800-122 • Cyber-Security in Today's K-12 Environment, Council of Great City Schools
	Data Breach			
	• Security Incident Response Policy • Cyber Insurance Policy		Security incident response plan, inclusive of procedures for identifying, containing, mitigating, reporting and communicating about security incidents.	Questions to ask: • Does the district need/have a policy requiring (or requiring a vendor) to have cyber insurance? If so, are there coverage thresholds?

	cont'd from above			*Guidance and Resources* • Data Breach Response Training Kit and Exercise (PTAC) • Data Breach Response Checklist (PTAC) • Data Security and Breach Notification Best Practice Guide (Kentucky) • Data Security Guide (NSBA/COSA) • CoSN brief on Cyber Insurance • CoSN Privacy Toolkit (see section titled, "Contracts and Terms of Service") (CoSN) *Example Communication* • Frederick County Public Schools (MD) Example of communication surrounding a data breach, including FAQ, sample letter, details on identity theft and risk mitigation. Your communications may vary depending on the nature of the particular incident. Your incident response communications should be written in close consultation with counsel and align with your legal requirements.
	Device Management/Security Policy		Device Security Standards Procedure for Lost Device	*Questions to ask:* • Consider if and when it is appropriate and legal to require certain password standards, security configurations, and the ability to enable lost-device tracking on staff or student-owned devices, and how administrative activation of this (or any other remote monitoring feature) will be managed and audited.
	Disaster Recovery Plan			
	Disaster Recovery and Business Continuity Policy		Disaster recovery plan, inclusive of checklists, internal communications requirements, testing standards and schedules.	*Guidance and Resources* • CoSN Technology Recovery Checklist *(members only resource)*

CoSN is grateful to the following sponsors for their support of this initiative:

CDW·G Clever its learning Microsoft PowerSchool

Consortium for School Networking 1325 G St, NW, Suite 420, Washington, DC 20005