Data Security & Privacy

Educational Technology Service

Genesee Valley
Wayne-Finger Lakes

Objectives

- Introduction
- Overview of Laws & Regulations
- Best Practices For Protecting Data
- Online Educational Services
- Additional Resources

Districts Manage Data In Multiple Systems

Student Information

Special Education

Human Resources

Cafeteria Management

Transportation

Learning Management

Online Services and Mobile Apps

…and many more

What data are we protecting?

- Demographics
- Enrollment
- Attendance
- Discipline
- Disability
- Free and Reduced Lunch
- English Language Learner
- Individual Education Programs
- Local Assessment Scores
- NYS Assessment Scores
- Course Grades
- Career and Technical Education
- Graduation and Diploma
- Human Resources
- Annual Professional Performance Review
- Student Learning Objectives

…and more

What are the challenges?

- The more we rely on technology, the more privacy is threatened
- New technology & Services = More New threats
- Laws continue lag technology
- Data is very valuable
- Privacy is PERSONAL

Overview of Laws & Regulations

Educational Technology Service

Genesee Valley Wayne-Finger Lakes

Family Education Rights and Privacy Act FERPA

Background	Federal law enacted in 1974 to protect student education records, or personally identifiable information (PII) from student education records, from unauthorized disclosure.
Applies To	Schools that receive funds under any program administered by the U.S. Secretary of Education
Key Provisions	Parents have the right to access their children's education records, the right to seek to have the records amended, and the right to consent to disclosure. Parents also have the right to file a complaint with the U.S Department of Education.
Additional Info	When a student turns 18 years old, or enters a postsecondary institution at any age, FERPA rights transfer from the parents to the student (they become an *eligible student*).

http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa101slides.pdf

FERPA
Personally Identifiable Information (PII)

Personally identifiable information (**PII**) is a **FERPA** term referring to identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to directly or indirectly identify a student.

http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa101slides.pdf

Children's Online Privacy Protection Act

Background	Enforced by the Federal Trade Commission since 2000 to give parents control over information collected from young children online
Applies To	Operators of websites, online services and mobile applications
Key Provision	COPPA assures that children under 13 years of age do not share personal information on the Internet without the express approval of their parents.
Additional Info	COPPA rules were amended in 2013. The amendments, among other things, expand the definition of personal information, require data deletion and retention procedures, and clarify the direct notification requirements to parents.

Children's Online Privacy Protection Act

Website and online service providers must give parents:

- Notice before collecting personal information online from children (and obtain consent)
- The choice to consent to internal use of a child's information, but prohibiting disclosure to third parties (unless clearly defined as integral to the site or service)
- Access to their child's personal information and the ability to request deletion
- The opportunity to prevent further use or collection of a child's personal information

They must also:

- Post a comprehensive online privacy policy describing their information practice
- Meet certain data confidentiality, security and retention requirements

Children's Online Privacy Protection Act

https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Protection of Pupil Rights Amendment PPRA

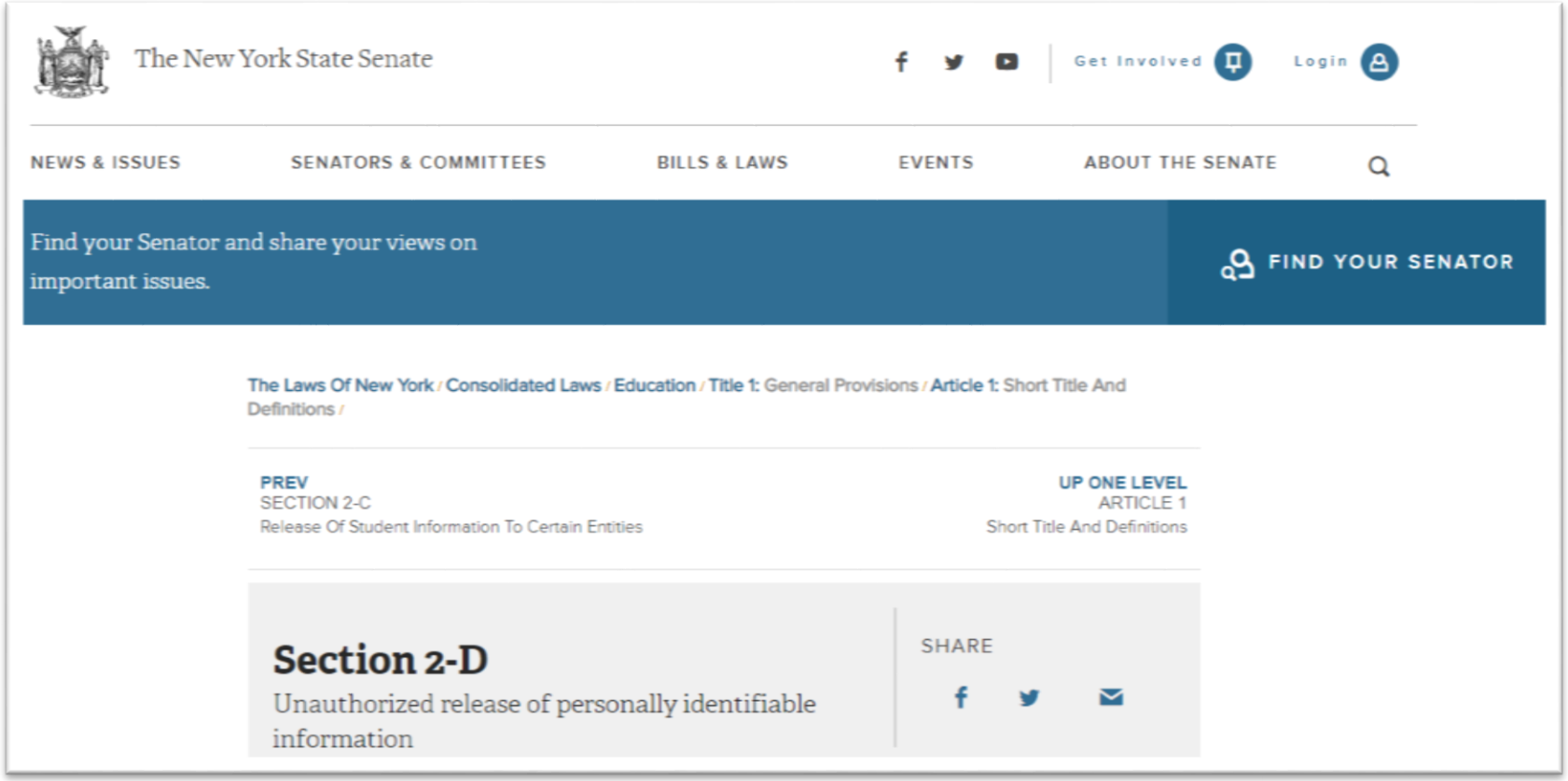
Background	Enacted in 1978 to protect the rights of students and parents of students in programs funded by the US Department of Education
Applies To	Any program funded by the United State Department of Education
Key Provisions	Schools and contractors must make instructional materials available for inspection by parents if those materials will be used in connection with an ED-funded survey, analysis, or evaluation that reveals certain kinds of personal information. Schools and contractors must obtain written parental consent before minor students are required to participate in any ED-funded survey, analysis, or evaluation
Additional Info	Districts must develop and adopt certain policies in consultation with parents and provide parents with notice of those policies and their rights under PPRA at least annually

NYS Education Law 2-d

Background	Created as part of the 2014 *Common Core Implementation Reform Act* to address the unauthorized release of PII from student, teacher and principal records
Applies to	Educational agencies (Districts, BOCES, NYSED) and third party contractors
Key Provisions	• Chief Privacy Officer Appointment (CPO) • Parents Bill of Rights for Data Privacy and Security • Data Collection Transparency and Restrictions • Data Security and Privacy Standards • Breach and Unauthorized Release Notification Procedures • Implementation and Enforcement

NYS Education Law 2-d

https://www.nysenate.gov/legislation/laws/EDN/2-D



Health Insurance Portability & Accountability Act - HIPPA

Background	Federal law enacted in 1996; the Privacy Law of HIPAA adopted in 2003 regulates the use and disclosure of Protected Health Information (PHI)
Applies To	Health Care Plans Health Care Clearinghouses, and every health care provider who electronically transmits health information in connection with certain transactions
Key Provisions	Mandates administrative, technical, and physical safeguards to ensure that individual health information remains private and secure Defines the circumstances in which an individual's protected heath information may be used or disclosed by covered entities
Additional Info	**Application to K-12 schools is limited as most student records, including health records, are education records covered by FERPA**

Best Practices For Protecting Data

Educational Technology Service

Genesee Valley
Wayne-Finger Lakes

Overview

- ✓ Data Inventory
- ✓ Privacy Officer
- ✓ De-identified data
- ✓ Passwords
- ✓ Email
- ✓ Workstation and File Security
- ✓ Mobile Computing Devices
- ✓ Technical Procedures
- ✓ Data Access and Permissions
- ✓ Verbal Communication
- ✓ Paper Copies
- ✓ Data Destruction

Overview

- ✓ Data Inventory
- ✓ Privacy Officer
- ✓ De-identified data
- ✓ Passwords
- ✓ Email
- ✓ Workstation and File Security
- ✓ Mobile Computing Devices
- ✓ Technical Procedures
- ✓ Data Access and Permissions
- ✓ Verbal Communication
- ✓ Paper Copies
- ✓ Data Destruction

Data Inventory

Address key questions about your data with a data inventory:

What systems do we have?

What data do they store?

What reports and exports are available?

Who are the users?

Sample Data Inventory

Data Type	Data Sub-Type	Source(s)	Currently Collected?	Responsibility	Where Accessed?	Who Has Access?
Student Achievement Data	State Assessment Results					
	District Assessments					
	Classroom Assessments					
Behavioral Data	Discipline Records					
	Attendance Records					
Teacher Use of Specific Instructional Strategies	Observations					
	Self-Assessments					
	Questionaire					
Teacher Participation in PD	Attendance Records					
	Survey/Reflection					
	Performance Eval Reports					
	Attendance Records					

Indirect Identification

Be mindful of indirect identification issues:

Subgroup	Percent Proficient
American Indian	83.4%
Asian	87.7%
Black	91.7%
Hispanic	81.0%
Two or More Races	0.00 %
White	79.2%

Workstation & File Security

Secure workstations and files:

- Lock your workstation when not in use
- Download and store documents with sensitive information on secure network drives - *not workstations!*
- Use only encrypted USB flash drives (if used at all)

Data Access & Permissions

Implement policy and procedure regarding user management and access that should be on a *"Need to Know"* basis:

- Review staff duties and roles annually
- Adjust permissions when job duties change
- Deactivate former employees accounts immediately
- Do not create generic accounts in systems
- Have processes and policies in place
- Review audit logs and reports

Privacy Officer

Determine who is responsible for the following data and privacy issues:

Leading a district security team

Educating staff on regulations, best practices and policy

Management and delivery of data

Maintaining information on agreements and contracts

Maintaining logs of users with access to PII

Documenting data collection processes

Acting as a contact for the public on privacy questions and concerns

Online Educational Services

Educational
Technology Service

Genesee Valley
Wayne-Finger Lakes

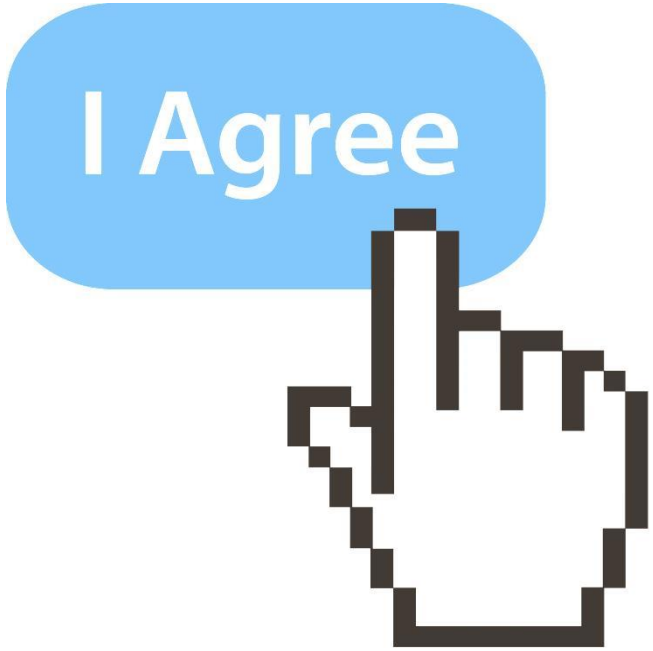
Online Educational Services - Issues

- Districts commonly contract out school functions and utilize online services.
- Traditional contracts involve a mutually agreed upon set of terms and a signed document between the parties.
- Many online services and mobile apps use a Terms of Service (TOS) agreement that only requires a user to click a button to accept (Click-Wrap Agreements)

Click Wrap Agreements

Terms of Service Agreements should be evaluated for items including:

- Definition of data, its use, and protections
- Marketing and Advertising
- Modification of Terms of Service
- Destruction of Data
- Security Controls



Contracts

Contracts should be evaluated for the following provisions:

- Security and data stewardship
- Data collection
- Data use, retention, disclosure, and destruction
- Data access
- Modification, duration, and termination
- Indemnification and warranty

Other Best Practices

Districts should…

- Establish policies and procedures to evaluate and approve proposed services
- Be transparent with parents and students
- Consider whether parental consent is appropriate
- Evaluate the use of services on a case-by-case basis to determine if the requirements of FERPA and other laws are met

Resources

Educational
Technology Service

Genesee Valley
Wayne-Finger Lakes

Resources

Protecting Student Privacy

The U.S. Department of Education is committed to student privacy. We administer the Family Educational Rights and Privacy Act (FERPA), and we provide technical assistance to help schools and school districts use best practices in their use and management of information about students. This site aims to assist stakeholders in protecting the privacy of students by providing official guidance on FERPA , technical best practices and the answers to Frequently Asked Questions. Responsibility for the Department's student privacy operations lies in the Office of the Chief Privacy Officer.

https://studentprivacy.ed.gov/

Protecting Student Privacy

U.S. DEPARTMENT OF EDUCATION

A Service of the Privacy Technical Assistance Center and the Family Policy Compliance Office

Search

RESOURCES • TRAINING • BROWSE BY AUDIENCE • FAQs

ABOUT US • CONTACT

FILE A COMPLAINT

Student Privacy 101:

STUDENT PRIVACY AT THE U.S. DEPARTMENT OF EDUCATION

The U.S. Department of Education is committed to student privacy. We administer the Family Educational Rights and Privacy Act (FERPA), and we provide technical assistance to


RESOURCES
TRAINING
BROWSE BY AUDIENCE
FAQs
K-12 School Officials
Parents and Students
Postsecondary School Officials
Early Childhood Educators
Vendors
Researchers
Student Privacy
STUDENT PRIVACY AT THE U.S
ON

Resources

Data Breach Response Training Kit

LAST UPDATED: JUNE 2017

DOWNLOAD DOCUMENT

Any organization with electronic records is vulnerable to security breaches, and education agencies are no exception. The PTAC Data Breach Scenario is one of a series of exercises intended to assist schools, districts, and other educational organizations with internal data security training.

The *Password* Data Breach interactive exercise is aimed at district management and provides a simulated response to a district-level data breach. Over the course of 1-2 hours, this customizable exercise leads participants through a scenario involving a breach of student information and other personally identifiable information. The exercise focuses on the processes, procedures, and skills needed to respond. The package includes three parts: Facilitator's Guide, PowerPoint Slides, and Exercise Handouts.

Over the course of 1-2 hours, this customizable exercise leads participants through a scenario involving a breach of student information and other personally identifiable information. The exercise focuses on the processes, procedures, and skills needed to respond. The package includes three parts: Facilitator's Guide, PowerPoint Slides, and Exercise Handouts.

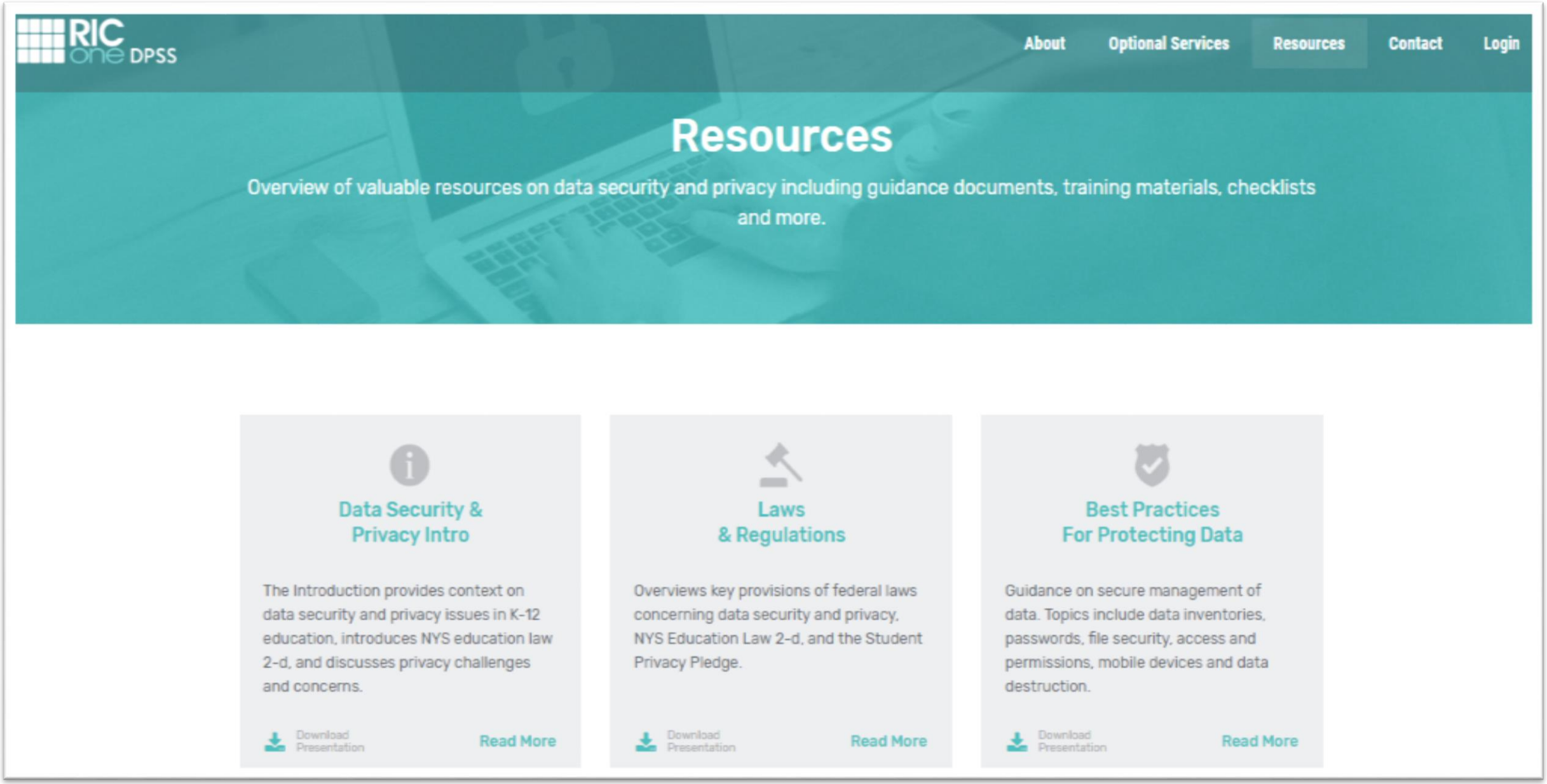
https://studentprivacy.ed.gov/resources/data-breach-response-training-kit

Resources

NYS RIC Data Security and Privacy Resource Center

The NYS RIC Data Security and Privacy Resource Center is an effort to inform the educational community about issues and best practices related to protecting student, teacher and principal data.

https://riconedpss.org/resources


RIC one DPSS
About
Optional Services
Resources
Contact
Login
Resources
Overview of valuable resources on data security and privacy including guidance documents, training materials, checklists and more.
Data Security & Privacy Intro
The Introduction provides context on data security and privacy issues in K-12 education, introduces NYS education law 2-d, and discusses privacy challenges and concerns.
Download Presentation
Read More
Laws & Regulations
Overviews key provisions of federal laws concerning data security and privacy, NYS Education Law 2-d, and the Student Privacy Pledge.
Download Presentation
Read More
Best Practices For Protecting Data
Guidance on secure management of data. Topics include data inventories, passwords, file security, access and permissions, mobile devices and data destruction.
Download Presentation
Read More

Resources

Consortium for School Networking (COSN)

The Consortium for School Networking (COSN) is a professional association for district technology leaders. Focus areas include Instruction, Leadership & Vision, and IT management.

www.cosn.org

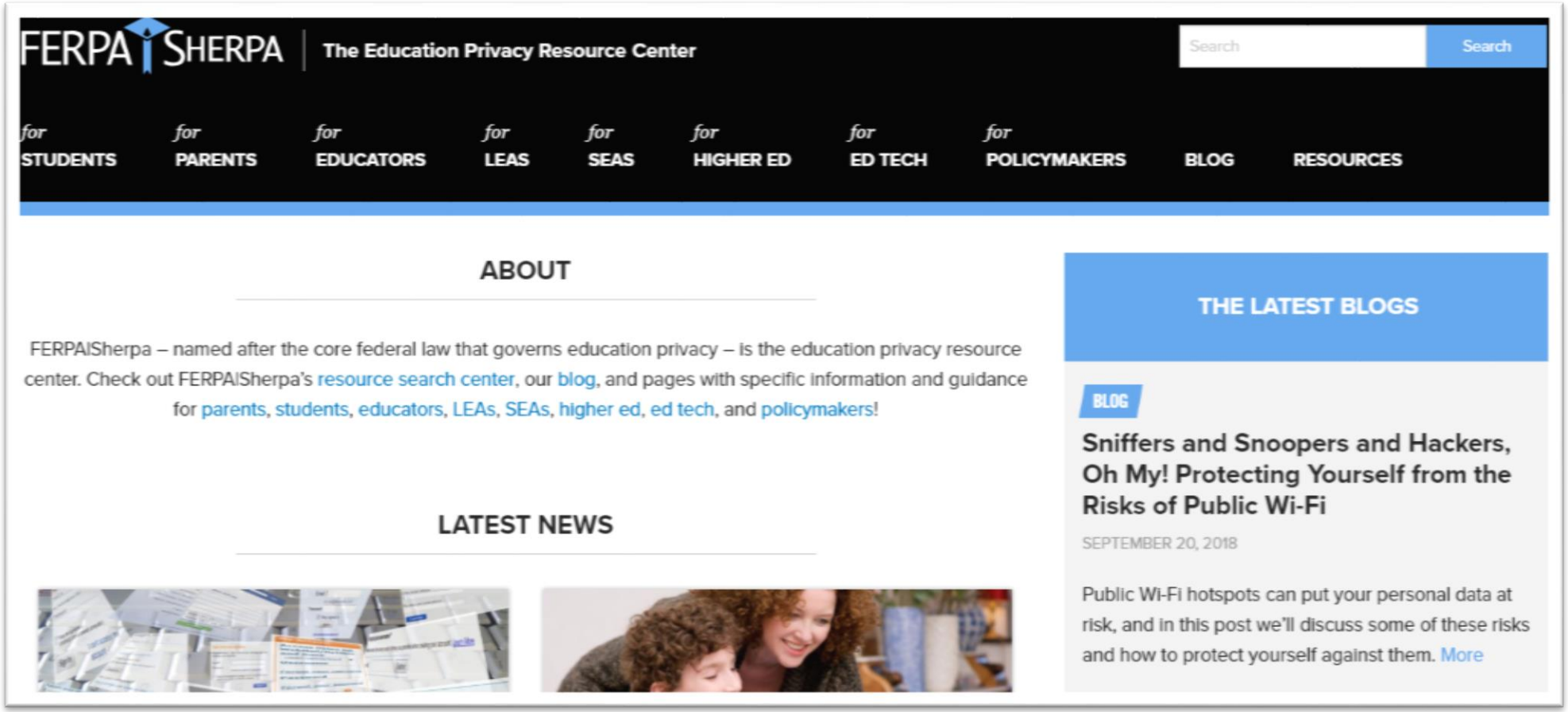
Resources

FERPA SHERPA

FERPA SHERPA is a project of the *Future of Privacy Forum*. It provides service providers, parents, school officials and policymakers with easy access to materials to guide responsible use of student's data.

ferpasherpa.org

Resources


FERPA SHERPA
The Education Privacy Resource Center
Search
Search
for STUDENTS
for PARENTS
for EDUCATORS
for LEAS
for SEAS
for HIGHER ED
for ED TECH
for POLICYMAKERS
BLOG
RESOURCES
ABOUT
FERPASherpa – named after the core federal law that governs education privacy – is the education privacy resource center. Check out FERPASherpa's resource search center, our blog, and pages with specific information and guidance for parents, students, educators, LEAs, SEAs, higher ed, ed tech, and policymakers!
LATEST NEWS
THE LATEST BLOGS
BLOG
Sniffers and Snoopers and Hackers, Oh My! Protecting Yourself from the Risks of Public Wi-Fi
SEPTEMBER 20, 2018
Public Wi-Fi hotspots can put your personal data at risk, and in this post we'll discuss some of these risks and how to protect yourself against them. More

Resources

Student Privacy Pledge

he Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA) introduced a Student Privacy Pledge to safeguard student privacy regarding the collection, maintenance, and use of student personal information. The commitments are intended to concisely detail existing federal law and regulatory guidance regarding the collection and handling of student data, and to encourage service providers to more clearly articulate these practices.

https://studentprivacypledge.org/

Resources

New York State EDUCATION DEPARTMENT

www.nysed.gov

http://www.nysed.gov/student-data-privacy/student-data-privacy-education-law