PlayWell, LLC

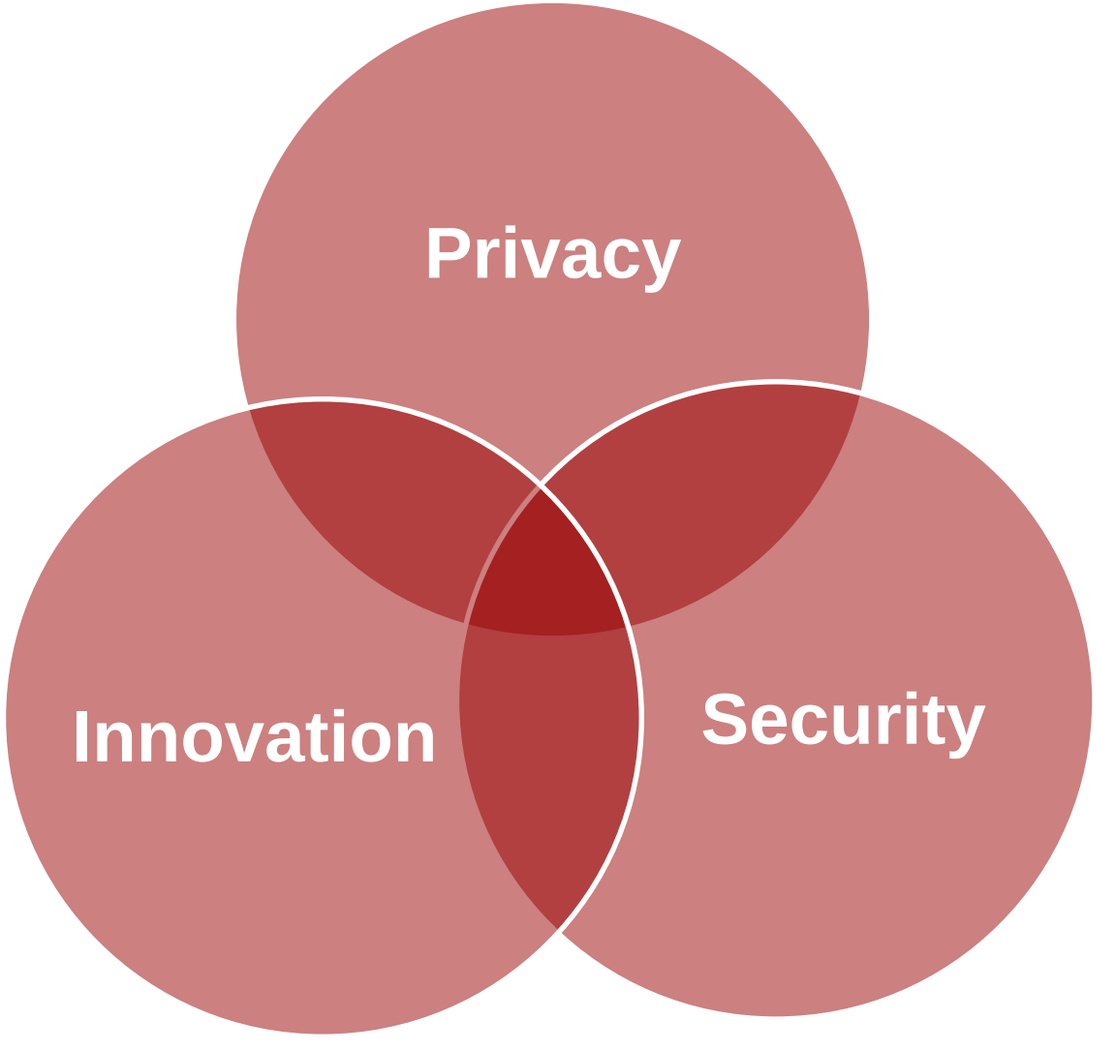
Getting Started with Student Data Privacy

About PlayWell

- Full-service compliance consulting
  - Technology assessments, policy development, training, communications
    - Schools, districts, education technology providers
  - Expertise in education and entertainment industry compliance
  - Backed by 25 years of compliance leadership and management experience with major media organizations
  - GDPR, FERPA, COPPA, PPRA, state student data privacy laws, marketing regulation, compliant innovation
  - Virtual Chief Privacy Officer & Data Protection Officer

How Comfortable Are You Being Uncomfortable?

What's Your Approach to Managing Risk?


Privacy
Innovation
Security

Why Does Privacy Matter?

- Inherent responsibility to provide a safe environment
- Repercussions:
  - Financial penalties
  - Regulatory action
  - Litigation
  - Reputational harm
- Building trust in the community

Protecting the privacy and security of student data is part of every school system's fundamental responsibility to protect students from harm.

Responsibility for bringing appropriate technology into the school system and for protecting the privacy and security of student data is yours.

Data Privacy 101: Key Privacy Concepts

- Fair Information Practices Principles
  - Transparency
  - Individual Participation
  - Purpose Specification
  - Data Minimization
  - Use Limitation
  - Data Quality and Integrity
  - Security
  - Accountability and Auditing

US Data Privacy Regulation

- Federal Trade Commission:
  - Section 5 of the FTC Act
    - Prohibits “unfair or deceptive acts or practices”
- Sector rules:
  - Family Educational Rights and Privacy Act (FERPA)
  - Children’s Online Privacy Protection Act (COPPA)
  - Protection of Pupil Rights Amendment (PPRA)
- State regulation
- District rules and community norms

Student Data Privacy Today

- Significant scrutiny around technology used in schools
  - 500+ student data privacy bills introduced across the states since 2013
    - ✓ 120+ new laws in 40 states
    - ✓ Focus on limiting advertising, data disclosure to third parties, increasing parental rights, data deletion, data security, transparency and accountability

How Did We Get Here?

- FERPA Updates
  - Why is data management allowed to be outsourced?
  - Are there federal protections in place?
  - Is vendor compliance monitored?
- Fordham Clip Study
  - Critical picture of lax school district management and control over cloud computing service providers.
  - Lack of basic contracts with vendors
  - Overt statutory violations
- inBloom
  - $110MM in Gates and Carnegie Foundation Funding
  - 9 states sign up; advocates question privacy; 8 states drop out
  - inBloom closes its doors

Advocacy Activity

- Criticism of self-regulatory efforts
  - Publicizing security flaws and technology assessment programs
- Growing “opt out” movement

Privacy Laws: A Closer Look

Family Educational Rights and Privacy Act

FERPA

- US Department of Education's Family Educational Rights and Privacy Act
  - Applies to education agencies & institutions that receive federal funding
  - Gives parents right to access educational records
  - Protects PII from unauthorized disclosure by educational institutions
  - Requires consent to share PII unless an exception applies

Education Records

- Education records: include any records, files, or documents that contain information directly related to a student and that are maintained by or for an educational agency or institution.
- Disclosure of personally identifiable information from education records not allowed without prior parental consent or consent from the eligible student (18+)

Personally Identifiable Information

- Includes, but is not limited to:
  - Student's name
  - Name of the student's parent or other family members
  - Address of the student or the student's family
  - Personal identifier such as a social security number or biometric record
  - Other indirect identifiers, such as the student's date or place of birth, and mother's maiden name
  - Other identifiers that alone or in combination could lead "a reasonable person in the school community" to identify a student

Directory Information

- Includes student education records generally considered not to be:
  - Harmful or
  - Invasion of privacy if disclosed
    - ✓e.g., name, address, phone number, date/place of birth, participation in official recognized activities and sports, and dates of attendance
- Schools must define directory information and allow parents and eligible students to opt out of sharing of those records

Access Rights

- Parents and eligible students:
  - Must be given the opportunity to inspect and review the student's education records
    - ✓Access must be provided within a "reasonable time"
  - May seek correction of inaccurate, misleading information

Exceptions to Consent Requirement

- Consent not required for disclosure of education records to third party provider when that provider acts as a “school official”
  - Performs service/function for school for which it would otherwise use its own employees
  - Is under direct control of school with respect to use of the data
  - Uses data in manner consistent with school official
  - Does not re-disclose or use data for unauthorized purposes

Costs of Non-compliance

- Educational institutions: risk losing federal funding

- Third party providers: educational institution prohibited from giving access to education records to that third party for at least 5 year
  - State and emerging federal legislation imposes additional penalties

Privacy Laws: A Closer Look

Children's Online Privacy Protection Act

What is COPPA?

- Federal Trade Commission's Children's Online Privacy Protection Act (COPPA)
  - Intentions:
    - ✓Ensure parents control what data is collect from their child (defined as users under 13)
    - ✓Minimize online data collection from childre
    - ✓Transparency around data practices
    - ✓Reasonable security procedures

General Requirements

- Compliance requirements:
  - Obtain verifiable parental consent before collecting, using or disclosing a child's personal information
  - Allow parents to review child's data/request that it be deleted or prevent further collection of data
  - Post a prominently displayed, accurate privacy policy

Verifiable Parental Consent

- Obtain parental consent prior to collection of personal information

OR

- A school may provide consent in place of the parents when:
  - Data is only for the use and benefit of the school
  - Data is not used for other commercial purposes
- A contract with a school may be used as an indication of consent

Data Access

- Parents always have the right to:
  - Request to review data/categories of data that have been collected from their child
  - Request that data be deleted
  - Request that no further contact be made with their child
  - Approve collection, but not disclosure of their child's data

Costs of Noncompliance

- Vendor penalties:
  - Monetary fines
  - Deletion of data
  - Consumer education
  - Compliance training and audits
  - Public relations and consumer trust

26

Privacy Laws: A Closer Look

Protection of Pupil Rights Amendment

Surveys, Analysis and Evaluation

- Parental notice/opt-out/right of inspection
- Protected information
  - Politics
  - Religion
  - Mental health
  - Sexual behavior or attitudes
  - Illegal, anti-social, self-incriminating, demeaning behavior
  - Critical appraisals of close relations
  - Privileged relationships
  - Income

"We are one data breach away from reactive data security legislation that will disregard the interests of schools and industry."

- Congressional staffer

State Student Data Privacy Laws

Key Concepts

- Student data remains under direct control of school or district
- Expanded definitions of protected information
- Personal information may be used only for K-12 school purposes
- Third party data access must be strictly limited
- Marketing may not be targeted based on student data
- Parents have access rights
- Delete data when no longer serving school purpose
- Preserve security and integrity of the data

Costs of Non-Compliance

- Financial penalties
  - Civil penalties
  - Private rights of action
- Revocation of business license
- Personal liability

Building and Improving Your Compliance Program

Getting to Governance

- Consider not just what is legally allowed, but also what is right for the organization
- Protecting student data requires informed leadership setting expectations and championing the efforts
- A successful compliance program can not exist without training and engagement at all levels

What Do You Want to Do With Data?

Start Where You Are

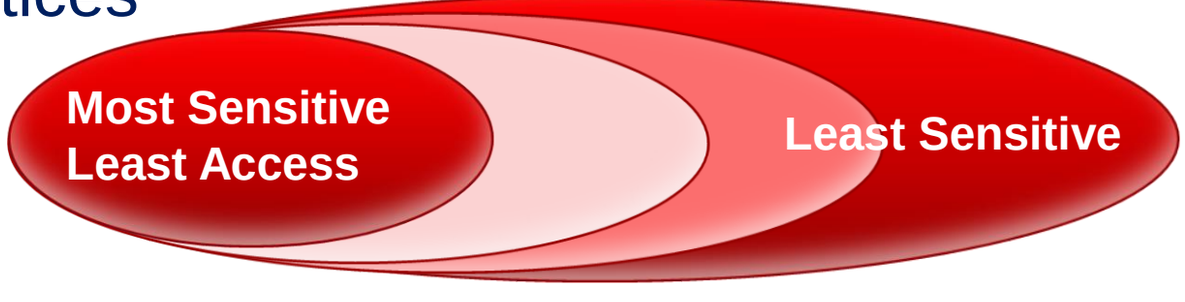
- Data inventory
- Data classification
- Data and system mapping
- Policy review
- Privacy impact assessment
  - Assess current policies and practices
    - Benchmark against legal requirements and district norms
- What technology is used?
- What data is collected?
- Why?
- Who has access?
  - Review data collection, use, sharing, retention and destruction

Cleaning Up the Gaps

- Prioritize by risk
- Remediation
  - Resources
    - Time
    - Finances
    - Manpower
    - Knowledge

Security Fundamentals

- Physical, technical and administrative safeguards
  - Physical barriers to data storage
  - Firewalls, encryption, authentication
  - Vulnerability scanning, monitoring and remediation
  - Rule and role-based access
  - Data retention and deletion policies and practices



Vendor Basics

- Technology assessment
  - Privacy policy
  - Terms of Use and/or written contract
- Contract safeguards
  - Direct control
  - Data remains your property
  - PII only used for K-12 purposes
  - PII shared only for the purpose of providing the services
  - Security safeguards/breach notification and support
  - Process for providing parent access

Policy Development

- How do you implement legal requirements and district norms?
  - What are the procedures you want your teams to follow
    - Bringing technology into the classroom
    - Data access
    - Password protocols
    - Responding to an incident
  - How are people held accountable?

Education and Training

- Legal requirements, policies, roles and responsibilities
- Authority for disclosing/sharing data
- Procedures for bringing technology into the classroom
- Understanding types of situations that create risks and mitigation procedures
- Creating a privacy culture
- Governance and accountability
- Transparency and communications

Creating a Governance Structure

Questions?

PlayWell, LLC

The Compliance Consultancy

Linnette Attai, President & Founder

Linnette@PlayWell-LLC.com +1 917-485-0353

www.PlayWell-LLC.com Facebook.com/PlayWellLLC @PlayWell_LLC