How to Ensure Data Privacy and Security in Schools Protecting Student Data and Privacy

Safeguard access in a remote and blended learning world
Presenters

Dr. Tina Barrios
Assistant Superintendent
Information Systems & Technology
Polk County Schools

George Perreault
Chief Academic Officer
ClassLink
Agenda

- Introduction
- What Should Vendors be Doing?
- How Should Districts Protecting Data?
- How Does ClassLink Help?
State Student Privacy Laws

42 States Have Passed 128 Laws Since 2013*

*160+ laws mentioning student privacy were passed since 2013, but the map above only includes laws that are primarily about student privacy or had significant student privacy provisions.

https://ferpasherpa.org/state-laws
The World has Changed

- Technology has changed how we live
- Most people are unsafe online
- Online danger looks different
- Knowledge is the best defense
What data must be protected?

- Data related to our students
- Data related to our students' families
- Data related to our staff
- Data related to our district
Personally Identifiable Information (PII)

- Any data that could potentially identify a specific individual
- PII can be sensitive or non-sensitive
- Non-sensitive PII includes data from public records, websites, etc.
- Non-sensitive PII can be transmitted unencrypted without harm
- Sensitive PII includes biometric information, medical info, SS #s, etc.
- Sensitive PII disclosure could be harmful to individuals
- Sensitive PII should be encrypted at rest and in transit
What types of data are typically collected?

- first & last name
- username
- email address
- student ID number
- grade level
- school enrollment
- homeroom

- parent/guardian name
- parent/guardian email
- district ID
- school ID
- state ID number
- class enrollments
- teacher names
What types of data are typically collected?

*Demographics*

- Gender
- Date of Birth
- Place of Birth
- Ethnicity or Race
PURCHASING POLICIES AND PROCEDURES
FOR LOCAL EDUCATIONAL AGENCIES

SCHOOL BOARD OF POLK COUNTY, FLORIDA

NON-DISCLOSURE AND DATA SECURITY AGREEMENT ADDENDUM
FOR INSTRUCTIONAL PROGRAMS AND MATERIALS
AND RELATED SERVICES
Welcome to the PURE process app

In order to enhance the focus of research and evidence based materials used with all students in Polk County Public Schools and to ensure that the products and professional learning provided by consultants are focused on district priority professional learning needs, all external providers of professional learning must complete the P.U.R.E. (Purchasing and Utilizing Resources Effectively) review process. This process is used to ensure that instructional materials and programs provided by external consultants and vendors are aligned with Florida Standards and the Strategic Plan of Polk County Public Schools.

All equipment, software, and technology service-related items must be reviewed and approved through the District’s Product Integration Evaluation (PIE) process, which is embedded within the PURE process. Vendors are prohibited from advertising, demonstrating, and/or showing non-PIE-approved equipment, software, and technology services to school-based personnel.

Vendors are NOT permitted to contact school personnel prior to P.U.R.E. approval. Doing so could place the approval of the program in jeopardy. During district adoption process for Instructional Materials, Polk County is a CLOSED school district.

If you are school board employee, please login to make an internal request, or review any request assigned to you.

Please pick a menu item on the left to get started! If there is no menu, try clicking the icon in the upper left to expand the menu or try maximizing the window.
P.U.R.E. - (Purchasing and Utilizing Resources Effectively) review process.

**Approval Levels**

- Direct Supervisor
- Content Area Associated with the product request
- Purchasing Manager confirmation of appropriate content area
- Assessment and Accountability
- Vendor Completes Program and Materials application
- Purchasing manager reviews application
- Vendor completes Product Integration Evaluation (PIE)
- Purchasing reviews PIE
- Vendor signs, scans and uploads Non-Disclosure agreement
- Purchasing reviews NDA
- Legal reviews NDA
- Curriculum Director approval
- Technology integration approval
- Purchasing reviews and approves technology integration
- Added to PURE list
Progress of Carnegie Learning FL High School Math Solution - Algebra 2 w/Honors

This progress bar shows every step of the PURE process and what step the product is on. The green circles indicate a step that has been completed. The blue circle is the product's current step. The grey circles have yet to be completed. A red circle indicates that the product expired or was rejected at that step. Not every step is required for every product. A step with a green circle but without a date indicates that step was not necessary for this product.
**Current Step:** Approval from curriculum directors

<table>
<thead>
<tr>
<th>Date Completed</th>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/28/2021</td>
<td></td>
<td>Initial request to review submitte</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approval from the submitter's di</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Content area &quot;Other&quot; is evaluate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approval from the content area c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Purchasing manager's confirmat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approval from AAE</td>
</tr>
</tbody>
</table>
Privacy Experts?

- Teacher
- Room Mom
- PTSA
Rethink Security Training

- Traditional awareness training, lacks effectiveness
- Fear has been overplayed
- Phishing without personal context, is not helpful
- You must speak human not tech
How Are You Protecting Your Data?
Risk Assessment

- Risk assessment - the starting point of cybersecurity
- Provides a roadmap to reducing and managing risk
- CoSN Risk Assessment powered by S2
  - Free
  - Entry level
  - K12 education specific
  - Aligns with NIST 800-53, CISA Top 18
  - Available publicly to members and non-members
  - Kept intentionally short – 3 questions per category

- [www.securitystudio.com](http://www.securitystudio.com)
Security and Data Privacy Policies

- Acceptable Use Policy
- Incident Response Policy & Procedure
- Incident Response Communication Plan
- Change Management Policy
- Network Firewall Policy
- Systems Development Life Cycle Policy
- System Configuration Standards
- Business Continuity Plan
- Acceptable Encryption Policy

- Data Backup Policy
- Information Logging Policy
- Password Policy
- Privacy Policy
- Disposal Policy
- Security Awareness Training Policy
- Vendor Risk Management Policy
- Mobile Device Policy
How Are You Protecting Your Data?

- Assess your cybersecurity preparedness
- Provide cybersecurity training for district personnel
- Develop strong security policies
- Protect your accounts
  - Use strong passwords
  - Change passwords often
  - Use multi factor authentication for sensitive accounts
  - Do not use password recovery with weak challenge responses
- Practice online safety
Multi-Factor Authentication

- Adds another layer of protection (in addition to username/password)
- Requires that a user provides multiple factors to validate their identity
- Factors used typically consist of some combination of two of three things:
  - Something you KNOW
  - Something you HAVE
  - Something you ARE
# Multi-Factor Authentication Options in ClassLink

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>ClassLink Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Something you know</strong>&lt;br&gt;(secret knowledge)</td>
<td>Any method where the user provides additional secret information.&lt;br&gt;e.g. image selection</td>
<td>ClassLink currently provides options for image selection.</td>
</tr>
<tr>
<td><strong>Something you have</strong>&lt;br&gt;(confidential possession)</td>
<td>Any method that requires the a secure token.&lt;br&gt;e.g. SMS text, Google Authenticator, Microsoft Authenticator, Duo MFA, RSA SecureID devices, Yubico YubiKey, Google Titan Key, solutions based on FIDO standard</td>
<td>ClassLink currently integrates with Google, Microsoft and Duo Authenticators through Universal 2nd Factor (U2F). ClassLink currently provides system architecture for supporting various hardware options. SMS texts are Time-based One-Time Passwords (TOTP).</td>
</tr>
<tr>
<td><strong>Something you are</strong>&lt;br&gt;(biology)</td>
<td>Any method that requires the receipt of biometric information.&lt;br&gt;e.g. ClassLink Faces, Apple FaceID, BioSig-ID</td>
<td>ClassLink currently provides facial recognition and system architecture for supporting biometric validation from third parties.</td>
</tr>
</tbody>
</table>
# Multi-Factor Authentication Best Practices

<table>
<thead>
<tr>
<th>Type</th>
<th>Form</th>
<th>Students</th>
<th>Teachers</th>
<th>Users with elevated permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Something you know</strong></td>
<td><strong>Challenge/ Response</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td><strong>Pin</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td><strong>Image select</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td><strong>Something you have</strong></td>
<td><strong>SMS text</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td><strong>Mobile auth app</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td><strong>Hardware fob</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Something you are</strong></td>
<td><strong>Fingerprint</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td><strong>Facial recog (IR)</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Security Do Now

- Take the CoSN Risk Assessment
  - [www.securitystudio.com/cosn](http://www.securitystudio.com/cosn)
- Understand MFA and develop a security plan
- Ongoing security training and awareness
- Develop a list of questions to ask all vendors
- Develop an action plan based on vendor answers
Questions to Ask Vendors

- How will you be securing our data?
- Do you have a Data Privacy Agreement?
- Do you offer secure single sign-on ability?
  - OAuth2, SAML, LTI, OpenID
- Do you use private servers for each district, or is data co-mingled?
- What data is collected, and for what purpose?
- Which industry standards are used for data interchange?
  - OneRoster, EdFi
- Do you conduct regular security audits using independent auditors?
- Do you perform regular independent penetration tests?
What Should Vendors be Doing?
Vendors Need to Ensure...

- Confidentiality
- Integrity
- Availability
Vendor Best Practices to Protect Data

- Data ownership - all PII is the property of the district
- Districts are in control of their data, and use classlink tools to share data with educational vendors of their choice
- Capture the minimum data required to ensure satisfactory operation of the system
- Private Cloud
- Secure single sign-ons
- Penetration testing
- Cyber Insurance
**OVERIDES**

OrgSourcedids

- Default

No modification to orgSourcedids

**OPTIONAL FIELDS**

- userIds
- identifier
- sms
- agentSourcedIds
- password

**METADATA FIELDS**

- metadata.job_titles

**REQUIRED FIELDS**

- sourcedId
- dateLastModified
- orgSourcedIds
- username
- firstName

middleName
email
phone
grades

metadata.primaryOrg
status
enabledUser
role
givenName
Optional Fields

- birthDate
- americanIndianOrAlaskaNative
- blackOrAfricanAmerican
- white
- hispanicOrLatinoEthnicity
- stateOfBirthAbbreviation
- publicSchoolResidenceStatus
- sex
- asian
- nativeHawaiianOrOtherPacificIslander
- demographicRaceTwoOrMoreRaces
- countryOfBirthCode
- cityOfBirth

Metadata Fields

There are no metadata fields within the Demographics collection.

Required Fields

- sourcedid
- dateLastModified
- status
How Does ClassLink Protect Your Data?

- Protection
  - Employees bound by non-disclosure agreements
  - Internal data management policies & procedures
  - Limitations on access to personal data
  - Data encryption in transit & at rest
  - Data systems monitoring
  - Incident response plans
  - Safeguards to ensure data is not accessed by unauthorized individuals
How Does ClassLink Protect Your Data?

- **Disposal of data**
  - Permanent disposal of personal data after termination of contract or no longer needed

- **Notification**
  - ClassLink promptly notifies affected customers of security breach resulting in authorized release of personal data, restores integrity of data systems as soon as possible

- **Full Range of Security Policies**
  - Establishes guidelines for security compliance
Security Audits and Certifications:

- SOC 2 Type II Audit
- ISO 27001 Audit
- CSA Star Audit
- iKeepSafe Certification
- EU Privacy Shield
- Student Privacy Pledge
ISO 27001 Audit

- International Organization for Standardization (ISO)
- ISO is an independent, non-governmental, international organization that develops standards for quality, safety, and efficiency of products, services, and systems
- ISO 27001 developed to help protect information in a systematic way
- Introduces the adoption of an Information Security Management System (ISMS)
- Goal is to protect Confidentiality, Integrity, and Availability
- Easily recognized all around the world
SOC 2 Type II Audit

- Service Organization Control (SOC)
- Developed by the American Institute of CPAs (AICPA)
- Audit designed for service providers storing customer data in the cloud.
- Requires companies to establish and follow strict information security policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.
Developed by the Cloud Security Alliance (CSA)
A rigorous third-party independent assessment of the security of a cloud service provider.
The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix.
Three levels of certification
- Level 1 - Self assessment
- Level 2 - Third-Party Certification
- Level 3 - Continuous Auditing for High Risk Environments
Trust but Verify

- FERPA, COPPA, GDPR Compliance
- Student Privacy Pledge
- Student Data Privacy Consortium (SDPC)
- Classlink.com/privacy

- Internal/External Penetration Testing
- iKeepSafe.org Audit
- Audits: SOC2, CSA STAR, ISO 27001
- Cyber Insurance
Get Back to Learning: in 24 hours - https://youtu.be/jXSETibpCRg

- Brian Nagel, Assistant Director of Technology for Haverhill Public Schools says when his district was hit by a ransomware attack, having ClassLink in place helped them get teachers and students back to learning in just 24 hours.

Douglas Russell - Director of Technology,
djrussell@haverhill-ps.org
Brian Nagel - Asst. Director of Technology,
bnagel@haverhill-ps.org
Resources

● FBI Cyber Attack Report
  ○ https://us-cert.cisa.gov/ncas/alerts/aa20-345a

● CoSN Risk Assessment
  ○ www.securitystudio.com/cosn

● K12 Cyber Incident Map
  ○ https://k12cybersecure.com/map/
Resources

- **National Data Privacy Agreement**
  - https://privacy.a4l.org/national-dpa/

- **State privacy laws**
  - https://ferpasherpa.org/state-laws

- **SIIA Student Privacy Pledge**
  - https://studentprivacypledge.org/
Resources

- **FERPA**

- **COPPA**

- **CIPA**

- **GDPR**
  - https://eugdpr.org/

- **EU Privacy Shield**
  - https://www.privacyshield.gov/welcome
Resources

- CoSN Cybersecurity
  - www.cosn.org/cybersecurity

- ClassLink Privacy
  - https://www.classlink.com/privacy

- ClassLink Security
  - https://www.classlink.com/security

- SOC2 Type II

- ISO 27001
  - https://www.iso.org/isoiec-27001-information-security.html

- CSA Star
  - https://cloudsecurityalliance.org/star/