WDE

School District Policy Guidelines

For the Collection, Access, Privacy, Security, and Use of Student Data

Updated 2024

Purpose

In the ever-evolving landscape of technology, it's crucial that Wyoming school districts adopt strong, current policies and processes to safeguard student data. This document reflects the latest best practices in cybersecurity, privacy, and compliance, and aligns with federal and state laws, including the Family Educational Rights and Privacy Act (FERPA) and other applicable regulations.

In 2017, W.S. 21-2-202 (a)(xxxvii) (A-E) required the Wyoming Department of Education to collaborate with the Department of Enterprise Technology, the Department of Audit, and school districts to develop guidelines for managing student data. School districts must develop and implement their own data security and privacy policies, using these guidelines as a framework.

This document provides updated guidelines based on current cybersecurity and data privacy frameworks, standards, and practices from organizations, including:

- National Institute of Standards and Technology (NIST).
- International Organization for Standardization (ISO).
- Center for Internet Security (CIS).
- Wyoming Department of Enterprise Technology Services (WY ETS).
- Wyoming Office of the Chief Information Officer (WY OCIO).

Guidelines

1. Data Collection and Minimization

To ensure transparency and data protection, districts should consider:

- Transparency: Publish a list of student data elements collected on the district's public website.
- Data Minimization: Eliminate the collection of Social Security Numbers (SSNs) whenever possible. Collect only the minimum necessary personal information to fulfill authorized educational purposes.
- Consistency: Ensure consistent data entry procedures across all applications, such as using legal names and implementing strict input validation to maintain data accuracy.
- Encryption of Data: Never send student or staff data via unencrypted email or other unsecured channels. Use secure protocols like TLS, HTTPS, or S/MIME for email transmission. Use established file transfer protocols for bulk data interchange (e.g., Secure FTP).

2. Authorization and Authentication Mechanisms

Passwords

- Enforce unique, strong passwords that are at least 12 characters long, combining uppercase and lowercase letters, numbers, and symbols. Encourage the use of passphrases and password managers.

- Implement Multi-Factor Authentication (MFA) for all accounts accessing sensitive data to provide an extra layer of protection.
- Enforce regular password updates and prohibit sharing or writing down passwords.

Permissions

- Use the Principle of Least Privilege (POLP) to ensure users only have the minimal access necessary to perform their job functions.
- Implement automated systems to revoke access immediately when an employee leaves the organization or changes roles.
- Limit the use of administrator accounts, using them only for essential tasks like installing or updating software.

Session Management

- Require automatic session timeouts after a period of inactivity (recommended: 15 minutes) and absolute session timeouts to minimize risk.
- Ensure applications provide mechanisms for users to actively close their sessions after use.

3. Administrative, Physical, and Logical Security Safeguards

Administrative Security

- Maintain written policies governing the collection, access, duplication, and dissemination of Personally Identifiable Information (PII).
- Require staff, volunteers, and contractors to sign confidentiality agreements with documented enforcement.
- Perform regular internal audits and monitoring systems that handle student data, including login attempts, access logs, and data usage.

Physical Security

- Lock workstations and secure areas with sensitive data. Implement automated screen locks after inactivity to prevent unauthorized access.
- Use secure disposal methods, such as shredding paper records or securely wiping digital data, when it is no longer needed.
- Secure server rooms and limit access to authorized personnel only.

Logical Security

- Regularly review and update firewall rules, conduct logging, and monitor network activities.
- Implement strict user account management protocols, such as deactivating accounts immediately upon staff exit and conducting periodic reviews of access levels.
- Prohibit the sharing of system and application accounts and credentials.
- Use end-to-end encryption for data in transit and at rest (AES-256 recommended for at-rest data).
- Create strict policies on the use of removable media (USB drives, external hard disks) to mitigate risks of data leaks.

4. Mobile Device Management

- Require auto-lock and password protection (or biometric security) on all mobile devices with access to district data.
- Implement Mobile Device Management (MDM) solutions to enable remote wipe and lock capabilities for lost or stolen devices.
- Prohibit taking district devices out of the country unless pre-approved and ensure all devices have encryption and up-to-date software installed.

5. Employee Training and Awareness

- Ensure all employees have access to data security and privacy policies and are required to complete training upon hire and at regular intervals thereafter.
- Conduct phishing simulations and other cybersecurity awareness exercises to help staff recognize potential security threats.
- Include specific guidelines on password security, safe email practices, and how to identify suspicious links and attachments in training materials.

6. Data Encryption

- Data in Transit: Always use secure communication protocols (e.g., TLS/SSL, sFTP) when transmitting sensitive data, particularly over third-party systems.
- Data at Rest: Encrypt stored student data using industry-standard encryption methods (e.g., AES-256) to prevent unauthorized access.
- Secure Email: Prohibit sending sensitive student data through unencrypted email and implement secure email tools like PGP or S/MIME for sensitive communications.

7. Data Governance - Privacy and Security Compliance

- Ensure compliance with FERPA and other relevant privacy regulations, such as the Children's Internet Protection Act (CIPA), Children's Online Privacy Protection Act (COPPA), Protection of Pupil Rights Amendment (PPRA), and HIPAA (where applicable).
- Data Quality & Accuracy: Establish clear standards for data collection, ensuring consistent and valid information for reporting and decision-making.
- Access & Accountability: Define who has access to student data and monitor usage to prevent unauthorized access while maintaining transparency for stakeholders.
- Perform annual privacy audits to ensure compliance and offer regular refresher training on privacy regulations.
- Contract and Data Sharing Agreements: Execute written agreements that comply with FERPA requirements when sharing student PII with third parties, ensuring contracts have the reason the data is being shared, the expectation that it will not be used for other purposes, and a process for destruction of the data after the contract ends.
- Utilize resources and services provided by student privacy protection organizations such as the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) and the Access 4 Learning (A4L)/ Community Student Data Privacy Consortium (SDPC).

8. Privacy and Security Maturity Models

- Consider adopting CIS Implementation Groups or the NIST Cybersecurity Framework, which provide structured guidance for developing privacy and security maturity through comprehensive standards that improve governance and security practices.

- Identify, assess, and mitigate data risks as part of an ongoing risk management process.
- Ensure compliance with regulatory requirements by reviewing and updating data governance policies.
- Conduct periodic reviews and updates of data policies to promote continuous improvement.
- Implement technical safeguards such as encryption and access controls to protect sensitive data.

9. Risk Assessment

- Conduct annual risk assessments with leadership and staff to identify vulnerabilities and evaluate the security posture of applications and key IT infrastructure.
- Assess risks related to the confidentiality, integrity, and availability of student data.
- Prioritize mitigation efforts based on the likelihood and potential impact of identified risks.

10. Incident Response and Breach Notification

- Develop a comprehensive incident response plan to include:
  - Incident Classification: Prioritize incidents based on severity and potential impact, enabling quick escalation for more severe cases.
  - Incident Response Planning: Define a step-by-step incident response protocol, identifying roles and responsibilities for each team member.
  - Breach Containment: Take immediate actions to contain a breach, such as isolating affected systems and halting data flow, to prevent further exposure.
  - Breach Notification: Develop procedures to notify affected parties and relevant authorities, including parents and staff, in compliance with regulations like FERPA, and as per federal and state laws.
  - Post-Incident Review & Mitigation: Conduct a root cause analysis to prevent future incidents, implementing improved security measures and training where needed.
  - Documentation: Maintain detailed records of each incident, including response actions, communications, and system updates, for compliance and continual improvement.
- Incident Identification & Monitoring: Establish systems to detect unusual activity or unauthorized access to data, such as through network monitoring and automated alerts.
- Conduct regular tests to ensure readiness.

11. Data Retention and Destruction

- Adhere to Wyoming records retention schedules and develop policies for electronic data retention.
- Ensure student-level data is securely deleted after the retention period, with names and other identifying information removed from data used for long-term analysis.
- Use secure data destruction methods (e.g., digital shredding) for both paper and electronic records.

12. Emergency Operations Plan (EOP) and Business Continuity Plan (BCP)

- Develop both an Emergency Operations Plan (EOP) and a Business Continuity Plan (BCP)
- Conduct a risk assessment to identify potential threats and impacts on school operations.
- Define critical functions that need to be maintained or restored during disruptions.
- Allocate resources to ensure personnel and technology are prepared for response and recovery.
- Develop communication protocols for effective internal and external coordination during emergencies.
- Establish safety procedures for evacuations, sheltering, and crisis management.
- Conduct regular training and drills to prepare staff for emergency response and recovery efforts.

13. Backup and Disaster Recovery

- Implement regular data backups and store them in secure, off-site locations.
- Perform routine disaster recovery drills to ensure data can be restored in the event of a system failure or security breach.
- Ensure that backup systems are protected with the same level of security as operational systems.

By adopting these updated guidelines, districts can enhance student data protection, comply with relevant laws, and proactively address evolving digital security threats.

Document Review/Revision History Table

Revision Number	Approved Revision Date	Summary of Changes	Next Review Date
1.0	9/25/2017	Initial Document	11/22/2027
2.0 1	1/22/2024	Modernized to current Standards and Best Practices, updated formatting	11/22/2027