LEA Model: Employee Security and Privacy Training Policy

Purpose: In order to minimize the risk of human error and misuse of information, {*Insert name of LEA*} provides a range of training opportunities for all staff using educational data.

All {INSERT NAME OF LEA} board members, employees, and contracted partners must sign and obey the {INSERT NAME OF LEA} Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.

All {INSERT NAME OF LEA} board members, employees, and contracted partners also must sign and obey the {INSERT NAME OF LEA} Employee Data Sharing and Confidentiality Agreement, which describes appropriate uses and the safeguarding of student and educator data.

All current {INSERT NAME OF LEA} board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 90 days of the adoption of this rule. New {INSERT NAME OF LEA} board members, employees, and contracted partners are required to complete the training within 30 days of their start date. This training is mandatory for continued access to {INSERT NAME OF LEA} 's network.

Additionally, {INSERT NAME OF LEA} requires a targeted Security and Privacy Training for Researchers and Evaluators for specific groups within the agency that collects, stores, and shares data. The Student Data Manager will identify these groups.

Participation in the training as well as a signed copy of the Employee Data Sharing and Confidentiality Agreement, will be annually noted in the Employee performance portal by supervisors. Supervisors and the board secretary will annually report all {INSERT NAME OF LEA} board members, employees, and contracted partners who do not have these requirements completed to the IT Security Manager.

Security and Privacy Fundamentals Training Curriculum (2017-2018)

Purpose: This training provides updated guidance to {INSERT NAME OF LEA} board members, employees, and contracted partners concerning compliance with state and federal privacy laws and best practices in this ever-changing environment.

Responsibility: The Chief Privacy Officer and the IT Security Manager will determine training curriculum for all {INSERT NAME OF LEA} board members, employees, and contracted partners.

- Introduction
    - Why we need information security training.
    - Real life examples
- Privacy
    - Our Goal is to Protect Student Data
    - What is PII
    - What is FERPA
    - What is COPPA
    - What is HIPPA
    - What is the Utah Student Data Privacy Act
    - What disclosures am I required to make
- Security Practices and Procedures
    - Physical Security
    - Accounts
    - Passwords
    - Copying Protected Data
    - Web Sites
    - Phishing, spear phishing, and vishing
    - Backups
    - Data Breach Response

Security and Privacy Training for Researchers and Evaluators Curriculum (2017-2018)

Purpose: This training provides updated guidance to {INSERT NAME OF LEA} board members, employees, and contracted partners concerning compliance with state and federal privacy laws and best practices in this ever-changing environment.

Responsibility: Data and Statistics Coordinator will determine the annual training topics for these targeted groups. Training for these groups will not be less than 8 hours school year.

- Ethical and professional standards for protecting educational data privacy
- Data redaction, suppression, masking techniques
- Reporting standards for multiple audiences
- Encryption requirements for data sharing