

Esperanza Elementary

Employee System Security and Privacy Training Policy

Purpose: In order to minimize the risk of human error and misuse of information, Esperanza Elementary provides a range of training opportunities for all staff using educational data.

All Esperanza Elementary board members, employees, and contracted partners must sign and obey the Esperanza Elementary Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.

All Esperanza Elementary board members, employees, and contracted partners also must sign and obey the Esperanza Elementary Employee Data Sharing and Confidentiality Agreement, which describes appropriate uses and the safeguarding of student and educator data.

All current Esperanza Elementary 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 Esperanza Elementary 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 Esperanza Elementary network.

Additionally, Esperanza Elementary 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.

Security and Privacy Fundamentals Training Curriculum 2017-2018

Purpose: This training provides updated guidance to Esperanza Elementary 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 Esperanza Elementary board members, employees, and contracted partners.

Introduction

- Why we need information security training
- Examples

Privacy

- Our Goal: Protect Student Data
- PII
- FERPA
- COPPA
- HIPPA
- 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

Revised 09/28/2017

