

Walden School Policy

Information Technology Security



Walden School takes seriously the obligation to ensure the security of the school's computer equipment, systems, and networks so that the sensitive data is maintained securely.

POLICY

The School will protect sensitive data, including personally identifiable student data, in accordance with school needs and state and federal law. Applicable state and federal law includes but is not limited to the Utah Student Data Protection Act, the Utah Family Educational Rights and Privacy Act, Utah Administrative Code Rule R277-487 Public School Data Confidentiality and Disclosure, the federal Family Educational Rights and Privacy Act, and the Government Records Access and Management Act.

Utah Administrative Code Rule R277-487 requires the School to, among other things, have an Information Technology Systems Security Plan that addresses the following:

1. System Administration
2. Network Security

3. Application Security
4. Endpoint, Server, and Device Security
5. Identity, Authentication, and Access Management
6. Data Protection and Cryptography
7. Monitoring, Vulnerability, and Patch Management
8. High Availability, Disaster Recovery, and Physical Protection
9. Incident Responses
10. Acquisition and Asset Management
11. Policy, Audit, and E-Discovery Training.

The Director, or the director's designee, shall establish, assure and regularly review the School Information Technology Systems Security Plan and its compliance with Utah Administrative Code Rule R277-487 and other applicable law.

The Information Technology Systems Security Plan shall work in conjunction with this policy and the School's Student Data Privacy and Security Policy, Data Governance Plan, metadata dictionary, and any other School policy, procedure, or plan concerning data privacy and security.

On an annual basis, the School shall provide appropriate training to its employees, aides, and volunteers regarding information technology security matters.