KARL G. MAESER PREPARATORY ACADEMY

TRUTH HONOR VIRTUE

Technology Security Policy

Approved: 12 June 2018

PURPOSE

The purpose of this policy is to ensure the secure use and handling of all data, computer systems and computer equipment by Maeser students, employees, and partners.

POLICY

Maeser will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.

All persons who are granted access to the school's network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of school devices and the network. When an employee or other user becomes aware of suspicious activity, s/he should immediately contact the school's IT Security Manager with the relevant information.

This policy also covers third party vendors/contractors that contain or have access to any of Maeser's sensitive data. All third party entities will be required to sign a Restriction on Use of Confidential Information Agreement before accessing Maeser systems or receiving sensitive data.

It is Maeser's policy to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and Privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the Utah State Board of Education. Maeser supports the development, implementation and ongoing improvement of a robust security system of hardware and software designed to protect Maeser's data, users, and electronic assets.

DEFINITIONS

Access: Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.

Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.

Computer network: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.

Computer property: Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

Encrypted data: Data/files requiring access to a secret key or password that enables decryption.

Personally Identifiable Information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered personally identifiable information.

Secured system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.

Sensitive data: Data that contains personally identifiable information.

System level: Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

PROCEDURE

SECURITY RESPONSIBILITY

Maeser shall appoint, in writing, an IT Security Manager responsible for overseeing school-wide IT security, to include development of school policies and adherence to the standards defined in this document.

TRAINING

The IT Security Manager shall ensure that all school employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all school employees.

The IT Security Manager shall ensure that all teachers provide annual student instruction on Cyber Security Awareness.

PHYSICAL SECURITY

Computer Security

All Maeser employees shall assist in protecting sensitive data by ensuring that computers used to access school systems are not left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. At the system level, automatic log off, locks and password screen savers will be used to assist employees in meeting this requirement.

Maeser shall utilize industry-standard systems and protocols to secure equipment and systems containing sensitive information in an effort to deter theft.

Server/Network Room Security

Maeser shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access controls to prevent unescorted access by unauthorized individuals.

Server rooms and telecommunication rooms/closets may only remain unlocked or unsecured when because of building design it is impossible to do otherwise or due to environmental problems that require the door to remain open.

Contractor access: Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor shall present a company issued identification card, and his/her access shall be confirmed directly by the authorized employee who issued the service request or by Maeser's Technology Department.

NETWORK SECURITY

Reasonable and appropriate network security protocols shall be implemented to regulate traffic moving between trusted internal (school) resources and external, untrusted (Internet) entities. Network transmission of sensitive data should enforce encryption where technologically feasible.

Network Segmentation

Maeser shall ensure that all untrusted and public access computer networks are separated from main school computer networks and shall utilize security policies to ensure the integrity of school computer networks.

Maeser will utilize industry standards and current best practices to segment internal computer networks based on the data they contain, to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

Wireless Networks

No wireless access point shall be installed on Maeser's computer network that does not conform with current network standards as defined by the IT Security Manager. Any exceptions to this must be approved directly in writing by the IT Security Manager.

Maeser shall scan for and remove or disable any unauthorized or unapproved wireless devices on a regular basis.

All wireless access networks shall conform to current best practices and shall utilize, at minimum, WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

Remote Access: Maeser shall ensure that any remote access with connectivity to the school's internal network is achieved using a school-approved secure. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the IT Security Manager.

ACCESS CONTROL

Maeser shall ensure that system and application access is limited to the lowest level of data or program access necessary to meet the user's legitimate educational need.

Authentication

Maeser shall enforce strong password management for employees, students, and contractors.

Password Creation: All system-level passwords must conform to specific password construction guidelines as defined by the IT Security Manager.

Password Protection: Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Password recovery systems must not hint at the format of a password (e.g., "my family name").

Authorization

Maeser shall ensure that user access is limited to the specific access necessary for the user's legitimate educational need. Where possible, segregation of duties will be utilized to control authorization access.

Maeser shall ensure that user access is granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

Accounting: Maeser shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.

Administrative Access Controls: Maeser shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

INCIDENT MANAGEMENT

Maeser's IT Security Manager shall designate systems to monitor and respond to IT related incidents to provide early notification of events as well as rapid response to and recovery from internal or external network or system attacks.

BUSINESS CONTINUITY

To ensure continuous critical IT services, Maeser's IT Security Manager will develop a business continuity/disaster recovery plan appropriate for the size and complexity of school IT operations.

Maeser shall develop and deploy a school-wide business continuity plan which shall include, at a minimum:

- *Backup Data*: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. At a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.
- *Secondary Locations*: Identification of a backup processing location.
- *Emergency Procedures*: A documented calling tree with emergency actions to include recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuing a full head count of all.

MALICIOUS SOFTWARE

Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware. Maeser shall install, distribute, and maintain spyware and virus protection software on all school-owned equipment, i.e. servers, workstations, and laptops. Maeser shall ensure that malicious software protection will include frequent update downloads, frequent scanning, and that malicious software protection is in active state (real time) on all operating servers/workstations. Maeser shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible. All computers must use the school-approved anti-virus solution. Any exceptions must be approved by the IT Security Manager.

INTERNET CONTENT FILTERING

In accordance with Federal and State law, Maeser shall filter internet traffic for content defined in law that is deemed harmful to minors.

Maeser acknowledges that technology based filters are not always effective at eliminating harmful content; for this reason, Maeser shall use a combination of technological and supervisory means to protect students from harmful online content.

Students shall be supervised when accessing the internet and using school-owned devices on school property.

Data Privacy

Maeser considers the protection of the data it collects on students, employees, and their families to be of the utmost importance.

Maeser protects student data in compliance with the Family Educational Rights and Privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 ("FERPA"), the Government Records and Management Act, U.C.A. §62G-2 ("GRAMA"), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 ("COPPA") and Utah Administrative Code R277-487 ("Student Data Protection Act").

Maeser shall ensure that access to student and employee records shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

Security Audit and Remediation

Maeser shall perform routine security and privacy audits in congruence with the school's Information Security Audit Plan.

School personnel shall develop remediation plans to address identified lapses that conform with the school's Information Security Remediation Plan.

Employee Disciplinary Action

Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and school policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment.

Student Disciplinary Action

Student Disciplinary Action shall be in accordance with applicable laws, regulations and school policies.