1. Purpose

The purpose of this policy is to ensure the secure use and handling of all Ogden Preparatory Academy (School) data, computer systems and computer equipment by School students, patrons, and employees.

2. Policy

2.1. Technology Security

2.1.1. It is the policy of the Ogden Preparatory Academy to support secure network systems in the School, including security for all Personally Identifiable Information (PII) that is stored digitally on School-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the School, its students, or its employees.

2.1.2. While data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be entirely preventable, the School will ensure that reasonable efforts will be made to maintain network security.

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

2.1.4. This policy and procedure also covers third party vendors/contractors that contain or have access to any Ogden Preparatory Academy critically sensitive data. All third party entities will be required to sign the Acceptable Use Agreement before accessing our systems or receiving information.

2.1.5. It is the policy of Ogden Preparatory Academy 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.

2.1.6. Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures included 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. Ogden Preparatory Academy supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect Ogden Preparatory Academy's data, users, and electronic assets.

3. Procedure

3.1. Definitions:

3.1.1. 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.

3.1.2. Authorization: Having the expressed 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.

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

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

3.1.5. 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.

3.1.6. 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.

3.1.7. 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.

3.1.8. Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

3.1.9. 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 Protected data

3.1.10. Security 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.

3.1.11. Sensitive data: Data that contains personally identifiable information.

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

3.2. Security Responsibility

3.2.1. Ogden Preparatory Academy Information Security Officer shall be responsible for overseeing School-wide IT security, to include development of School policies and adherence to the standards defined in this document.

3.2.2. Ogden Preparatory Academy shall designate jointly the IT Director and the Student Data Manager as the Information Security Officer.

3.3. Training

3.3.1. Ogden Preparatory Academy, led by the ISO, shall ensure that all School employees having access to sensitive information undergo annual security training which emphasizes personal responsibility for protecting student and employee information. - Training resources will be provided to all School employees.

3.3.2. Ogden Preparatory Academy, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

3.4. Physical Security

3.4.1. Computer Security

3.4.1.1. It is the policy of Ogden Preparatory Academy that any user's computer not be left unattended and unlocked, particularly when logged into sensitive systems or data including student or

employee information. Ogden Preparatory Academy shall use automatic log off, locks and password screen savers.

3.4.1.2. Ogden Preparatory Academy shall ensure that all equipment that contains sensitive information will be secured to deter theft.

3.4.2. Server/Network Room Security

3.4.2.1. Ogden Preparatory Academy shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school office areas. Access control shall be enforced using either keys, electronic card readers, or similar method with only those IT or other staff members having access necessary to perform their job functions are allowed unescorted access.

3.4.2.2. Telecommunication rooms/closets may only remain unlocked or unsecured when, due to building design or environmental problems, it is impossible to do otherwise.

3.4.3. Contractor access

3.4.3.1. Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and his/her access shall be confirmed directly by the IT Director or his/her designee.

3.5. Network Security

3.5.1. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (School) resources and external, untrusted (Internet) entities. All network transmission of sensitive data should enforce encryption where technologically feasible.

3.5.2. Network Segmentation

3.5.2.1. Ogden Preparatory Academy shall ensure that all untrusted and public access computer networks are separated from School computer networks and utilize security policies to ensure the integrity of those computer networks.

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

3.5.3. Wireless Networks

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

3.5.3.2. Ogden Preparatory Academy shall scan for and remove or disable any rogue wireless devices on a regular basis.

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

3.5.4. Remote Access

3.5.4.1. Ogden Preparatory Academy shall ensure that any remote access with connectivity to the School's internal network is achieved using the School's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Information Security Officer.

3.6. Access Control

3.6.1. System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.

3.6.2. Authentication

3.6.2.1. Ogden Preparatory Academy shall enforce strong password management for employees, students, and contractors.

3.6.2.2. Passwords

3.6.2.2.1. All system-level passwords must conform to the Ogden Preparatory Academy Password Policy.

3.6.3. Authorization

3.6.3.1. Ogden Preparatory Academy shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

3.6.3.2. Ogden Preparatory Academy shall ensure that user access should be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.

3.6.4. Accounting

3.6.4.1. Ogden Preparatory Academy shall maintain, for at least 90 days, audit and log files 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.

3.6.5. Administrative Access Controls

3.6.5.1. Ogden Preparatory Academy shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

3.7. Incident Management

3.7.1. Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

3.8. Business Continuity

3.8.1. Ogden Preparatory Academy's sensitive IT Services will be securely backed up with our business partners off site via cloud storage management. This data is backed up continuously and can be restored by the IT Director at any time. Ogden Preparatory Academy's Student Information System is managed by the Utah State Board of Education.

3.9. Malicious Software

3.9.1. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.

3.9.2. Ogden Preparatory Academy shall install, distribute, and maintain spyware and virus protection software on all school-owned equipment, i.e. servers, workstations, and laptops.

3.9.3. Ogden Preparatory Academy shall ensure that malicious software protection includes frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.

3.9.4. Ogden Preparatory Academy 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.

3.9.5. All computers must use the School approved anti-virus solution.

3.9.6. Any exceptions must be approved by the IT Director.

3.10. Internet Content Filtering

3.10.1. In accordance with Federal and State Law, Ogden Preparatory Academy shall filter internet traffic for content defined in law that is deemed harmful to minors.

3.10.2. Ogden Preparatory Academy acknowledges that technology based filters are not always effective at eliminating harmful content and due to this, Ogden Preparatory Academy uses a combination of technological means and supervisory means to protect students from harmful online content.

3.10.3. In the event that students take devices home, Ogden Preparatory Academy will provide a technology based filtering solution for those devices. However, parents and/or guardians are responsible to provide the supervision necessary to fully protect students from accessing harmful online content.

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

3.11. Data Privacy

3.11.1. Ogden Preparatory Academy considers the protection of the data it collects on students, employees and their families to be of the utmost importance.

3.11.2. Ogden Preparatory Academy 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").

3.11.3. Ogden Preparatory Academy shall ensure that employee records access 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.

3.12. Security Audit and Remediation

3.12.1. Ogden Preparatory Academy shall routinely audit its information business partners to verify information security.

3.13. 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 with Ogden Preparatory Academy.

Document History
Approved: 12/14/2017

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