CITY ACADEMY

City Academy's Mission *is to graduate responsible, informed citizens who have achieved their best academic success. We do this through distinctive teaching that is engaging, investigative and thought-provoking; close attention to each student's finest learning and personal progress; and involving students well in exploration of civic and current issues and in our city.*

CITY ACADEMY IT SYSTEMS SECURITY PLAN

Technology Security Policy

City Academy supports secure network systems, including security for all personally identifiable information (PII) that is stored on paper or digitally on school computers and networks. City Academy mitigates data threats that may harm the school, its students, or its employees. City Academy will make reasonable efforts to maintain network security, understanding that data loss can be caused by human error, hardware malfunction, or natural disaster, and may not be preventable.

When an employee or other user becomes aware of suspicious communication or unauthorized use of data, he or she will immediately contact the City Academy information security officer.

City Academy fully conforms 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 (FERPA), the Government Records and Management Act U.C.A. §62G-2 (GRAMA), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

City Academy will train staff and students regarding the importance of network security and best practices. The procedures associated with this policy are consistent with guidelines provided by and in accordance with Utah Education Network and the Utah State Board of Education. City Academy supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect our data, users, and electronic assets.

Procedures

1. Security Responsibility

City Academy appoints our IT manager as our student data manager responsible for overseeing data security, to include development of policies and adherence to the standards defined in this document.

2. Training

City Academy will ensure that all employees having access to sensitive information undergo annual data privacy training in August which emphasizes their personal responsibility for protecting student and employee information. Training resources will be provided to all employees.

City Academy will ensure that students are educated about cyber security and protection of their own data privacy.

3. Physical Security

City Academy will ensure that any user's computer is not left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Users will set up automatic log off and protect devices with strong passwords to enforce this requirement.

City Academy will ensure that all equipment that contains sensitive information will be secured to deter theft.

City Academy will ensure that server rooms and telecommunication rooms are kept locked, with access only by authorized personnel.

4. Network Security

Network perimeter controls will be implemented to regulate traffic moving between trusted City Academy resources and external, untrusted entities. All network transmission of sensitive data will enforce encryption where technologically feasible.

City Academy will ensure that all untrusted and public access computer networks are separated from main district computer networks and utilize security policies to ensure the integrity of those computer networks.

City 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.

No wireless access point shall be installed on City Academy's computer network that does not conform with current network standards as defined by the network manager.

City Academy will scan for and remove or disable any rogue wireless devices on a regular basis.

All wireless access networks will conform to current best practices and shall utilize at minimal WPA encryption for any connections.

5. Access Control

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.

City Academy will enforce strong password management for employees, students, and contractors.

- Do not share **information system passwords** with anyone. All passwords are to be treated as sensitive, confidential information.
- Do not insert information system passwords into email messages or other forms of electronic communication.
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

City Academy will ensure that user access to information systems be limited to only those specific access requirements necessary to perform their jobs, and that access to information systems is terminated and school-owned devices are returned when an employee leaves the school.

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

6. Incident Management

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.

7. Business Continuity

Student data and other sensitive files are backed up in the Cloud and protected by strong passwords. The server is backed up automatically at regular intervals.

8. Malicious Software

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

City Academy will install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.

City Academy will ensure that malicious software protection will include at least weekly update downloads and scanning, and that malicious software protection is in active state (real time) on all operating servers/workstations.

City Academy will 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.

9. Internet Content Filtering

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

City Academy acknowledges that technology based filters are not always effective at eliminating harmful content. City Academy therefore uses a combination of technological means and supervisory means to protect students from harmful online content.

In the event that students take devices home, City Academy will provide a technology based filtering solution for those devices. However, City Academy will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content.

Students shall be monitored when accessing the internet and using City Academy owned devices on school property.

10. Data Privacy

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

City Academy protects student data in compliance with FERPA, GRAMMA, 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).

City 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.

11. Security Audit and Remediation

City Academy shall perform routine security and privacy audits on at least a monthly basis.

School personnel shall develop remediation plans to address identified lapses that conforms with the school's information security remediation plan template.

12. Employee Disciplinary Actions

Any employee found to be in violation of City Academy's technology security plan or non-disclosure agreement may be subject to disciplinary action up to and including termination of employment with City Academy.