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 Data Governance Plan

Data Governance Committee Members: IT Systems Coordinator and City Academy Advisory Council
Student Data Manager: IT Systems Coordinator
Data Governance Committee Meetings: Annually

POLICY

Introduction

Protecting our student and staff privacy is an important priority at City Academy. We value the trust of our students, parents, and staff and are committed to maintaining strong and meaningful privacy and security protections.

This City Academy Data and Information Governance, Security, and Use document includes information regarding the Data and Information Governance Committee, the City Academy Data and Information Governance, Security, and Use Policy (DIGSU Policy), applicable Appendices, and Supplemental Resources.

The DIGSU Policy formally outlines how operational and instructional activity shall be carried out to ensure City Academy's data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it.

The City Academy DIGSU Policy shall be a living document. To make the document flexible, details are outlined in the Appendices. With the City Academy Board's approval, (1) the City Academy Data Governance Committee (CADGC) shall be the City Academy Advisory Council (CAAC) in collaboration with the City Academy Systems Administrator, and (2) the CADGC may recommend modifications to the Board concerning information in the Appendices in response to changing needs. All modifications shall be approved by the Board and posted on the City Academy school website.

I. PURPOSE

A. It is the policy of City Academy that data or information in all its forms--written, electronic, or printed--is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information.

B. The Data and Information Governance, Security, and Use (DIGSU) policies and procedures are documented and reviewed annually by the City Academy Data Governance Committee (CADGC).

C. City Academy conducts annual training on their data governance policy for faculty, staff, and students, and documents that training.

D. The terms "data" and "information" are used separately, together, and interchangeably throughout the policy. The intent is the same.

II. SCOPE

The City Academy Executive Director is authorized to establish, implement, and maintain data and information security measures. The policy, standards, processes, and procedures apply to all students and employees of City Academy, contractual third parties and agents of the school, and volunteers who have access to school data systems or data.

This policy applies to all forms of City Academy data and information, including but not limited to:

A. Speech, spoken face to face, or communicated by phone or any current and future technologies,
B. Hard copy data printed or written,
C. Communications sent by post/courier, fax, electronic mail, text, chat and or any form of social media, etc.,
D. Data stored and/or processed by servers, PC's, laptops, tablets, mobile devices, etc., and
E. Data stored on any type of internal, external, or removable media or cloud based services.

III. REGULATORY COMPLIANCE

City Academy will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. City Academy complies with all applicable regulatory acts including but not limited to the following:

A. Children's Internet Protection Act (CIPA)
B. Children's Online Privacy Protection Act (COPPA)
C. Family Educational Rights and Privacy Act (FERPA)
D. Health Insurance Portability and Accountability Act (HIPAA)
E. Payment Card Industry Data Security Standard (PCI DSS)
F. Protection of Pupil Rights Amendment (PPRA)

IV. RISK MANAGEMENT

A. A thorough risk analysis of all City Academy data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Executive Director. The risk assessment shall be used as a basis for plan development and implementation to mitigate identified threats and risk to an acceptable level.

B. The Executive Director or designee administers periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures are implemented that mitigate any identified threats by reducing the amount and scope of the vulnerabilities.

V. DATA CLASSIFICATION

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data are classified according to the most sensitive detail they include. Data recorded in several formats (e.g., source document, electronic record, report) have the same classification regardless of format.

VI. SYSTEMS AND INFORMATION CONTROL

Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems. All involved systems and information are assets of City Academy and shall be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

A. **Ownership of Software:** All computer software developed by City Academy employees or contract personnel on behalf of City Academy, licensed or purchased for City Academy's use is the property of City Academy and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.

B. **Software Installation and Use:** All software packages that reside on technological systems within or used by City Academy shall comply with applicable licensing agreements and restrictions and shall comply with City Academy's acquisition of software procedures.

C. **Virus, Malware, Spyware, Phishing and SPAM Protection:** Virus checking systems approved by the Systems Director are deployed using a multi-layered approach (computers, servers, gateways, firewalls, filters, etc.) that ensures all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. Users shall not turn off or disable City Academy protection systems or install other systems.

D. **Access Controls**: Physical and electronic access to information systems that contain Personally Identifiable Information (PII), Confidential information, Internal information and computing resources are controlled. To ensure appropriate levels of access by internal employees, a variety of security measures are instituted as recommended by the Systems Director and/or the City Academy Data Governance Committee and approved by the City Academy Board. Mechanisms to control access to PII, Confidential information, Internal information and computing resources include, but are not limited to, the following methods:

   1. **Authorization**: Access shall be granted on a "need to know" basis and shall be authorized by the Board with consultation from the Executive Director, Principal, immediate supervisor, or CADGC and with the assistance of the Systems Director. Specifically, on a case-by-case basis, permissions may be added in to those already held by individual users in the student management system, again on a need-to-know basis and only in order to fulfill specific job responsibilities, with approval of the Executive Director or Systems Director.

   2. **Identification/Authentication:** Unique user identification (user ID) and authentication

are required for all systems that maintain or access PII, Confidential information, and/or Internal Information. Users shall be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall NOT be shared.

3. **Data Integrity:** City Academy provides safeguards so that PII, Confidential, and Internal Information are not altered or destroyed in an unauthorized manner. Core data are backed up to a private cloud for disaster recovery. In addition, listed below are methods that are used for data integrity in various circumstances:
    a. transaction audit
    b. disk redundancy (RAID)
    c. ECC (Error Correcting Memory)
    d. checksums (file integrity)
    e. data encryption
    f. data wipes

4. **Transmission Security:** Technical security mechanisms are in place to guard against unauthorized access to data that are transmitted over a communications network, including wireless networks. The following features are implemented:
    a. integrity controls and
    b. encryption, where deemed appropriate

    Note: Only LEA-supported email accounts shall be used for communications to and from school employees, to and from parents or other community members, to and from other educational agencies, to and from vendors or other associations, and to and from students for school business.

5. **Remote Access:** Access into City Academy's network from outside is not allowed without explicit authorization from the Executive Director and Systems Director. Further, PII, Confidential Information and/or Internal Information that are stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the City Academy network. PII shall only be stored in cloud storage if said storage has been reviewed by the Executive Director, Systems Director, the City Academy Data Governance Committee, and approved by the Board.

6. **Physical and Electronic Access and Security:** Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals. At a minimum, staff passwords shall be changed annually.
    a. No PII, Confidential and/or Internal Information shall be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that are not approved by Executive Director, Systems Director, and City Academy Data Governance Committee.
    b. No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate Purchasing and Disposal of Electronic Equipment procedures.
    c. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.

E. Data Transfer/Exchange/Printing:

1. **Electronic Mass Data Transfers:** Downloading, uploading or transferring PII, Confidential Information, and Internal Information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be in accordance with this policy and be reviewed by the City Academy Data Governance Committee and approved by the Board. All other mass downloads of information shall be reviewed by the CADGC and/or Systems Director, approved by the Board and include only the minimum amount of information necessary to fulfill the request. A Memorandum of Agreement (MOA) shall be in place when transferring PII to external entities such as software or application vendors, textbook companies, testing companies, or any other web based application, etc. unless the exception is approved by the data governance committee.

2. **Other Electronic Data Transfers and Printing:** PII, Confidential Information, and Internal Information shall be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible shall be de-identified before use.

F. **Oral Communications:** City Academy's staff shall be aware of their surroundings when discussing PII and Confidential Information. This includes but is not limited to the use of cellular telephones in public areas. City Academy's staff shall not discuss PII or Confidential Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

G. **Evaluation:** City Academy requires that periodic technical and non-technical evaluations of access controls, storage, and other systems be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

H. **IT Disaster Recovery:** Controls shall ensure that City Academy can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the Executive Director, Risk Management Officer, and/or Systems Director for response to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages data or systems. The IT Disaster Plan shall include the following:

I.

1. A prioritized list of critical services, data, and contacts.
2. A process enabling City Academy's to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
3. A process enabling City Academy's to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
4. Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

VII. COMPLIANCE

A. This DIGSU Policy applies to all users of City Academy information including: employees, staff, students, volunteers, and outside affiliates. Failure to comply with this policy by employees, staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable City Academy procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with this policy by students may constitute grounds for corrective action in accordance with City Academy policies. Further, penalties associated with state and federal laws may apply.

B. Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:
    1. Unauthorized disclosure of PII or Confidential Information.
    2. Unauthorized disclosure of a log-in code (User ID and password).
    3. An attempt to obtain a log-in code or password that belongs to another person.
    4. An attempt to use another person's log-in code or password.
    5. Unauthorized use of an authorized password to invade student or employee privacy by examining records or information for which there has been no request for review.
    6. Installation or use of unlicensed, unapproved, or unauthorized software on City Academy technological systems.
    7. The intentional unauthorized altering, destruction, or disposal of City Academy information, data and/or systems. This includes the unauthorized removal from MBS of technological systems such as but not limited to laptops, internal or external storage, computers, servers, backups or other media, copiers, etc. that contain PII or confidential information.
    8. An attempt to gain access to log-in codes for purposes other than for support by authorized technology staff, including the completion of fraudulent documentation to gain access.