Genesee Community Charter School
at the Rochester Museum & Science Center
657 East Ave. ● Rochester, NY 14607 ● (585) 697-1960 ● www.GCCSchool.org

Genesee Community Charter School
Data Security and Privacy Policy

Purpose

This policy addresses The Genesee Community Charter School's (GCCS) responsibility to adopt appropriate administrative, technical and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems and information technology resources.

Policy Statement

It is the responsibility of GCCS:

1) To comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information.
2) To maintain a comprehensive Data Privacy and Security Program designed to satisfy its statutory and regulatory obligations, enable and assure core services, and fully support GCCS's mission.
3) To protect personally identifiable information (PII), and sensitive and confidential information from unauthorized use or disclosure.
4) To address the adherence of its vendors with federal, State and GCCS requirements in its vendor agreements.
5) To communicate its required data security and privacy responsibilities to its users and train its users to share a measure of responsibility for protecting GCCS's data and data systems.

Standard

GCCS will utilize the National Institute of Standards and Technology's Cybersecurity Framework
(NIST CSF) as the standard for its Data Privacy and Security Program.

Scope

The policy applies to all GCCS students, parents/guardians, consultants, and third-parties who receive or have access to GCCS' data and/or data systems ("Users').

This policy encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of GCCS, and it addresses all information, regardless of the form or format, which is created or used in support of the activities of GCCS.

This policy shall be published on the GCCS website and notice of its existence shall be provided to all Users.

Compliance

GCCS' Board of Trustees, School Leader, and Data Protection Officer are responsible for the compliance of their programs with this policy, related policies, and their applicable standards, guidelines and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and corrective practices will be adopted as applicable.

Oversight

GCCS' School Leader and Data Protection Officer shall report to the Board of Trustees on data privacy and security activities, the number and disposition of reported breaches, if any, and a summary of any complaints submitted pursuant to Education Law §2-d.

Data Privacy

1) Laws such as the Family Educational Rights Privacy Act (FERPA), NYS Education Law §2-d and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.
2) Data protected by law must only be used in accordance with law and regulation, and GCCS policies to ensure it is protected from unauthorized use and/or disclosure.
3) The GCCS administrative team will manage its use of data protected by law. This team will determine whether a proposed use of PII would benefit student needs. This team will also ensure that PII is not included in public reports or other public documents, or otherwise publicly disclosed, unless documented written consent is given.
4) No student data shall be shared with a third party without a written agreement that complies with state and federal laws and regulations. No student data will be provided to third parties unless it is permitted by state and federal laws and regulations. Third-party contracts must include provisions required by state and federal laws and regulation.
5) The identity of all individuals requesting PII, even where they claim to be a GCCS employee, student parent/guardian, eligible student or the data subject, must be authenticated by GCCS procedures.

6) It is GCCS' policy to provide all protections afforded to GCCS parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Act, and the federal regulations implementing such statutes. Therefore, GCCS shall ensure that its contracts require that the confidentiality of student PII be maintained in accordance with federal and state law and its policy.
7) Contracts with third parties that will receive or have access to PII must include a Data Privacy and Security Plan that outlines how the contractor will ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.

Incident Response and Notification

GCCS will respond to data privacy and security incidents in accordance with its Incident Response Policy. The incident response process will determine if there is a breach. All breaches must be reported to the Data Protection Officer or the School Leader. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student PII as defined by Education Law §2-d., or any GCCS sensitive or confidential data system that stores data, by a person not authorized to acquire, access, user or receive the data.

GCCS will comply with legal requirements that pertain to the notification of individuals affected by a breach or unauthorized disclosure of PII.

Acceptable Use Policy, User Account Password Policy and other Related School Policies

1) Users must comply with GCCS' Information Security Policy, which outlines the responsibilities of all users of GCCS information systems to maintain the security of the system and to safeguard the confidentiality of GCCS information.
2) Users must comply with the Acceptance Use of IT Resources Policy in using GCCS' resources. Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks in accordance with GCCS' mission and business functions.
3) Users must comply with the User Account Password Policy
4) All remote connections must be made through managed points-of-entry in accordance with the Data Privacy and Security Guidelines for Remote Work.

Training

GCCS Users must annually complete GCCS' information privacy and security training.

Board Approved December 9, 2020