Galway Central School District - DATA PRIVACY AND SECURITY POLICY

I. Purpose

This policy addresses Galway Central School District (GCSD)'s 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.

II. Policy Statement

It is the responsibility of GCSD:

(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 the Department's mission;
(3) to protect personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure;
(4) to address the adherence of its vendors with federal, state and SED requirements in its vendor agreements;
(5) to train its users to share a measure of responsibility for protecting SED's data and data systems;
(6) to identify its required data security and privacy responsibilities and goals, integrate them into relevant processes, and commit the appropriate resources towards the implementation of such goals; and
(7) to communicate its required data security and privacy responsibilities and goals and the consequences of non-compliance, to its users.

III. Standard

GCSD will utilize the National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST CSF or Framework) as the standard for its Data Privacy and Security Program.

IV. Scope

The policy applies to GCSD employees, and also to independent contractors, interns, volunteers ("Users") and third-party contractors who receive or have access to GCSD's data and/or data systems.

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

This policy, as implemented, shall ensure that every use and disclosure of personally identifiable information by GCSD shall benefit students and GCSD and shall ensure that personally identifiable information shall not be included in public reports or other documents.

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

V. Compliance

All Users 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 Users will be directed to adopt corrective practices, as applicable.

VI. Oversight

GCSD's Data Protection Officer shall annually report to its Board of Education on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint submitted pursuant to Education Law §2-d.

VII. 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 GCSD policies to ensure it is protected from unauthorized use and/or disclosure.

(3) GCSD has established a Data Protection Officer and a Data Privacy Committee to manage its use of data protected by law. The Data Protection Officer and the Data Privacy Committee will determine whether a proposed use of personally identifiable information would benefit

students and educational agencies, and to ensure that personally identifiable information is not included in public reports or other public documents, or otherwise publicly disclosed;

(4) No student data shall be shared with third parties 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 regulations.

(5) The identity of all individuals requesting personally identifiable information, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with GCSD procedures.

(6) It is GCSD's policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, required under the Family Educational Rights and Privacy Act, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, GCSD shall ensure that its contracts require that the confidentiality of student data or teacher or principal APPR data be maintained in accordance with federal and state law and this policy.

(7) Contracts with third parties that will receive or have access to personally identifiable information 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.

VIII. Incident Response and Notification

GCSD will respond to data privacy and security critical incidents in accordance with its **Data Breach and Cyber Incident Response Policy.** All breaches of data and/or data systems must be reported to the Data Protection Officer. All breaches of personally identifiable information or sensitive/confidential data must be reported to the Data Protection Officer. For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student, teacher or principal PII as defined by Education law §2-d, or any GCSD sensitive or confidential data or a data system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.

State and federal laws require that affected individuals must be notified when there has been a breach or unauthorized disclosure of personally identifiable information. Upon receiving a report of a breach or unauthorized disclosure, the Superintendent, Data Protection Officer, school attorneys, and other subject matter experts will determine whether notification of

affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay.

Parents, eligible students, teachers, principals or other staff of GCSD may file a complaint about breaches or unauthorized releases of student data and/or teacher or principal data. The complaint must be filed with GCSD in writing. Upon receiving such a complaint, GCSD will promptly acknowledge receipt of same, commence and investigation, and take any necessary precautions to protect personally identifiable information. Following its investigation, the GCSD shall provide the complainant with its findings no more than 60 calendar days from the receipt of the complaint. Should GCSD require additional time to relay its findings, or where the response may compromise security or impede a law enforcement investigation, GCSD shall provide the complainant with a written explanation that includes the approximate date when the GCSD anticipates that it will respond to the complaint.

IX. Acceptable Use Policy, Password Policy and other Related GCSD Policies

(1) Users must comply with the **Acceptable Use Policy** in using GCSD 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 GCSD missions and business functions (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the district or moved to another position.
(2) Users must comply with the **Password Policy**.
(3) Users must comply with all other Related GCSD Policies.

X. Training

All users of GCSD data, data systems and data assets must annually complete the information security and privacy training offered by the district. Information security and privacy training will be made available to all users. Employees must complete the training annually.

XI. Agreements with BOCES

GCSD may join an executed agreement between a board of cooperative educational services and a third-party vendor. Before GCSD joins any such agreement, GCSD, prior to joining, shall review any such agreement and shall ensure that the agreement complies with all confidentiality laws and implementing regulations, including, but not limited to, the Family Educational Rights and Privacy Act (FERPA) and Education Law § 2-d.