8635

DATA PRIVACY AND SECURITY POLICY

I. Purpose

This policy addresses the Corning-Painted Post Area School District's (the District) 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 the District:

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 District'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 District requirements in its vendor agreements; and
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 the District's data and data systems.

III. Standard

The District 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 District employees, interns, volunteers, and consultants, and third-parties who receive or have access to the District's 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 the District and it addresses all information, regardless of the form or format, which is created or used in support of the activities of the District.

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

Compliance

Department Administrators are responsible for the compliance of their programs and offices 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 program offices will be directed to adopt corrective practices, as applicable.

DATA PRIVACY AND SECURITY POLICY, Con't.

V. Oversight

The Data Protection Officer shall annually report to the Board of Education 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.

VI. 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 District policies to ensure it is protected from unauthorized use and/or disclosure.
3) The District has established a Data Privacy Committee to manage its use of data protected by law. The Data Protection Officer and the Data Privacy Committee will, together with program offices, 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 regulation.
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 District procedures.
6) It is the District'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, the District 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.

VII. Incident Response and Notification

The District 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. 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 District 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.

The District will comply with legal requirements that pertain to the notification of individuals affected by a breach or unauthorized disclosure of personally identifiable information.

DATA PRIVACY AND SECURITY POLICY

VIII. Acceptable Use Policy, User Account Password Policy and other Related District Policies

1) Users must comply with the District's Acceptable Use Policy, which outlines the responsibilities of all users of the District's information systems to maintain the security of the systems and to safeguard the confidentiality of the District's information.
2) Users must comply with the Acceptable Use of IT Resources Policy in using District 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 the District's 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 Remote Work and Telecommuting Policy.

IX. Training

All District Users must annually complete the District's information privacy and security training.

Ref: Education Law § 2-D
8 NYCRR Part 121
Family Education Rights and Privacy Act ("FERPA") 34 CFR Part 99
Children's Online Privacy Protection Act ("COPPA") 16 CFR Part 312
Protection of Pupil Rights Amendment 20 USC § 1232(g)

New: December 16, 2020