

**SUBJECT: Data Security and Privacy Policy in accordance with Education Law 2-d, Part 121**

## **I. Purpose**

This policy addresses Windsor Central School District's (Windsor CSD) 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 Windsor CSD:

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;
5. to train its users to share a measure of responsibility for protecting District 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. Program Standards and Alignment**

The Windsor CSD Data Privacy and Security Program aligns with the National Institute of Standards and Technology 's Cybersecurity Framework v 1.1 (NIST CSF).

#### **IV. Scope**

The policy applies to Windsor CSD employees, and also to independent contractors, interns, volunteers ("Users") and third-party contractors who receive or have access to District 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 shall be published on the Windsor CSD website and notice of its existence shall be provided to all employees and Users.

#### **V. Compliance**

All administrative employees are responsible for the compliance of their staff and 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 program offices will be directed to adopt corrective practices, as applicable.

#### **VI. Oversight**

Windsor CSD'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. Windsor CSD shall take steps to minimize its collection, processing and transmission of personally identifiable information.
3. Data protected by law must only be used in accordance with law and regulation and Windsor CSD policies to ensure it is protected from unauthorized use and/or disclosure. Windsor CSD shall not sell, use or disclose any personally identifiable information for marketing or commercial purposes, or facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party

to do so. Every use and disclosure of personally identifiable information shall be for the benefit of students and Windsor CSD.

4. The Chief Privacy officer and the Managed Technology Services Team 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;
5. 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.
6. 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 Windsor CSD's procedures.
7. It is Windsor CSD'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, Windsor CSD 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.
8. Contracts with third parties that will receive or have access to personally identifiable information must include a supplement to the parent's bill of rights, which shall be published on the Windsor CSD website and a signed waiver 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.
9. Except as required by law or regulation or in the case of enrollment data, Windsor CSD shall not report to NYSED juvenile delinquency records, criminal records, medical health records, or student biometric information.

## **VIII. Incident Response and Notification**

1. The District will respond to data privacy and security critical incidents in accordance with its Data Breach and Cyber Incident Response procedure. All breaches of data and/or data systems, 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 Windsor CSD 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.

2. 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 Data Protection Officer, Counsel and other subject matter experts will determine whether notification of affected individuals is required, and where required, effect notification in accordance with applicable laws and regulations.
3. Windsor CSD shall require that all complaints of breaches or unauthorized disclosures be submitted in writing.

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

1. Users must comply with the all acceptable use and internet policies in using the District's 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 (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the District.
2. Users must comply with the District password conventions and periodic password changes.
3. All remote connections must be made through managed points-of-entry that are overseen and secured by the South Central Regional Information Center.

**X. Training**

All users of department 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. No Right of Action**

Nothing contained in this policy or Windsor CSD's Data Privacy and Security Plan shall be construed as creating a private right of action against Windsor CSD.

BOE: 6/23/2020  
Adopted: 9/15/2020