Policy

PERSONNEL 4243

DATA SECURITY AND PRIVACY

I. Purpose

This policy addresses Jefferson Lewis Hamilton Herkimer Oneida BOCES' ("BOCES") 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 BOCES:

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 BOCES' 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 BOCES' requirements in its vendor agreements;
5. To train its users to share a measure of responsibility for protecting BOCES' 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

BOCES 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

1. The policy applies to BOCES employees, and also to independent contractors, interns, volunteers ("Users") and third-party contractors who receive or have access to BOCES' data and/or data systems.
2. 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 BOCES.
3. This policy shall be published on the BOCES' website along with the Parents Bill of Rights for Data Security and notice of its existence shall be provided to all employees and Users.

V. Compliance

The Chief Executive Officer and/or District Superintendent is responsible for the compliance of BOCES' 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.

VI. Oversight

The BOCES' Data Protection Officer shall annually report to the Board 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 BOCES policies to ensure it is protected from unauthorized use and/or disclosure.
3. BOCES will take steps to minimize collection, processing and transmission of PII.
4. BOCES has established a Data Governance Team to manage its use of data protected by law. The Data Protection Officer and the Data Governance Team will, together with program offices, determine whether a proposed use of PII would benefit students and educational agencies, and ensure that PII 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. BOCES will not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.
7. The identity of all individuals requesting PII, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with BOCES' procedures.
8. It is BOCES' 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, BOCES 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.
9. 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.
10. All third party contracts that will receive or have access to PII are required to comply with the BOCES Parent's Bill of Rights for Data Privacy and Security.

VIII. Incident Response and Notification

1. BOCES will respond to data privacy and security critical incidents in accordance with its Technology and Safety, Information Security Breach, Education Records, Student Technology and Safety policies and regulations.
2. All breaches of data and/or data systems will be reported by the Data Governance Team to the Data Protection Officer.
3. All breaches of PII 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 BOCES 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.
4. State and federal laws require that affected individuals must be notified when there has been a breach or unauthorized disclosure of PII. Upon receiving a report of a breach or

unauthorized disclosure, the Data Governance Team and other related professionals will determine whether notification of affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay.

IX. Technology and Safety and Student Technology and Safety Policies

1. Users must comply with the Technology and Safety and Student Technology and Safety polices and regulations in using BOCES resources.
2. 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 BOCES User Access Policy.
3. Accounts will be removed, and access will be denied for all those who have left the BOCES or moved to another department.
4. Users must comply with the password requirements as outlined in the Acceptable Use Policy.
5. All remote connections must be made through managed points-of-entry in accordance with the User Access Policy

X. Training

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

Jefferson-Lewis-Hamilton-Herkimer-Oneida Board of Cooperative Educational Services
Legal Ref: Education Law §2-d; NYCRR T. 8, Ch. II, Subch. E, Pt. 121; Family Educational Rights and Privacy Act; Individuals with Disabilities Education Act
Cross Ref: Policy 4240, 4242, 5050, 5250, 6001

Adopted: May 13, 2020