**Monroe 2-Orleans BOCES Policy**
**Series 5000 – Personnel**
**Policy #5261 – PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA – EDUCATION LAW 2-d**

BOCES will maintain the privacy and security of student data and teacher and principal data (hereinafter referred to as "PII") and will follow all applicable laws and regulations for the handling and storage of this data when disclosing or releasing the data.

BOCES will take steps to minimize the collection, processing, and transmission of PII. BOCES will not sell PII. BOCES will not use or disclose PII for any marketing or commercial purpose. BOCES will not facilitate, use or disclose PII to any other party for any marketing or commercial purposes.

Except as required by law or in the case of educational enrollment data, the BOCES will not report to NYSED the following student data elements:

a) Juvenile delinquency records;

b) Criminal records;

c) Medical and health records; and

d) Student biometric information.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student data or teacher or principal data by a person acting exclusively in the person's capacity as an employee of the BOCES.

## Data Protection Officer

BOCES designates Ray Miller, Supervising Manager, as the Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures required by Education Law Section 2-d and the Commissioner's Regulations. The Data Protection Officer is the main point of contact for data privacy and security.

## Data Privacy and Security Standards

BOCES will protect the privacy of PII by:

a) Reviewing whether the use and disclosure of PII benefits students and the BOCES by considering, among other criteria, whether the use and/or disclosure will:

   1. Improve academic achievement;

   2. Empower parents and students with information; and/or

   3. Advance efficient and effective program and academic operations.

b) Excluding PII in public reports and/or other public documents.

c) Affording all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents and/or eligible students.

**Monroe 2-Orleans BOCES Policy**
**Series 5000 – Personnel**
**Policy #5261 – PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA – EDUCATION LAW 2-d**

## Third-Party Contractors

BOCES will include in contracts with third-party contractors where PII is disclosed to the vendor in the course of doing business with the vendor language obligating the vendor to maintain the privacy and security of the PII in accordance with law, regulation and NIST Cybersecurity Framework, the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

The third-party contractor's data privacy and security plan must, at a minimum include the following:

a) Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract;

b) Specify the administrative, operational, and technical safeguards and practices in place to protect PII that the vendor will receive under the contract;

c) Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);

d) Specify how officers and/or employees of the third-party contractor and its assignees who have access to PII will receive training on the laws governing confidentiality of this data prior to receiving access;

e) Specify if the third-party contractor will utilize subcontractors and the plan to ensure the subcontractor protects PII;

f) Specify how the third-party contractor will identify breaches and unauthorized disclosures, and expediently notify BOCES;

g) Describe upon the termination or expiration of the contract whether, how, and when data will be returned to BOCES, transitioned to a successor contractor, deleted or destroyed;

h) Include a copy of the Parents' Bill of Rights for Data Privacy and Security which the contractor must sign;

i) Explain the technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

j) Agree to limit internal access to PII to only those employees or subcontractors that have legitimate educational interests;

k) Agree not to use the PII for any purpose not explicitly authorized in the contract;

l) Agree not to disclose any PII to any other party without the prior written consent of the parent or eligible student except:

    1. To authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with the BOCES or

2. As required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the Board, or the institution that provided the information, no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order.

m) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

n) Use encryption to protect PII in its custody while in motion or at rest; and

o) Will not sell PII, will not use or disclose PII for any marketing or commercial purpose; will not facilitate, use or disclose PII to any other party for any marketing or commercial purposes.

**Click-Wrap Agreements**

Periodically, BOCES staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

BOCES staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data unless they have received prior approval from the BOCES Data Protection Officer or designee.

**Parents' Bill of Rights for Data Privacy and Security**

BOCES will publish the Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. The Bill of Rights will be included with every contract or other written agreement it enters into with a third-party contractor where the third-party contractor will receive PII.

The Bill of Rights will state in clear and plain English that:

a) A student's PII cannot be sold or released for any commercial purposes;

b) Parents have the right to inspect and review the complete contents of their child's education record;

c) State and federal laws protect the confidentiality of PII, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred;

d) A complete list of all student data elements collected by the state is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234; and

e) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New

York 12234. Complaints may also be submitted using the form available http://www.nysed.gov/data-privacy-security/report-improper-disclosure

The Bill of Rights will also include supplemental information for each contract the BOCES enters into with a third-party contractor where the third-party contractor receives PII. The third party contractor will sign the Bill of Rights.

**Supplemental to the Bill of Rights**

The supplemental document to the Bill of Rights must include the following information:

a) The exclusive purposes for which the PII will be used by the third-party contractor, as defined in the contract;

b) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the PII will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations;

c) The duration of the contract, including the contract's expiration date, and a description of what will happen to the PII upon expiration of the contract or other written agreement;

d) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

e) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and whether data is encrypted and data privacy and security risks mitigated; and

f) Address how the data will be protected using encryption while in motion and at rest.

BOCES will publish on its website the supplement document to the Bill of Rights for any contract or other written agreement it has entered into with a third-party contractor that will receive PII. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the BOCES data and/or technology infrastructure.

**Right of Parents and Eligible Students to Inspect and Review Students' Education Records**

Consistent with the obligations under FERPA, parents and eligible students have the right to inspect and review a student's education record by making a request directly to the BOCES, see Policy 6320.

**Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data**

Parents have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. Parents, eligible students, teachers, principals, and other BOCES staff may file complaints with the BOCES about breaches or unauthorized releases PII as follows:

a) All complaints must be submitted to the Data Protection Officer in writing.

b) BOCES will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.

c) BOCES will provide the individual who filed the complaint with its findings within a reasonable period of time, but no more than sixty (60) calendar days from the receipt of the complaint.

d) If the BOCES requires additional time, or where the response may compromise security or impede a law enforcement investigation, the BOCES will provide the complainant a written explanation that includes the approximate date when the BOCES anticipates that it will respond to the complaint.

BOCES will maintain a record of all complaints of breaches or unauthorized releases of PII and the disposition in accordance with the Records Retention and Disposition Schedule LGS-01 (1988; rev. 2004).

**Reporting a Breach or Unauthorized Release**

BOCES will report every discovery or report of a breach or unauthorized release of PII to the NYSED Chief Privacy Officer no more than ten (10) calendar days after the discovery.

Each third-party contractor that receives PII will be required to notify the BOCES of any breach of security resulting in an unauthorized release of the PII in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, BOCES policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after the discovery of the breach.

BOCES will in turn notify the Chief Privacy Officer of the breach or unauthorized release of PII no more than ten (10) calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

**Investigation of Reports of Breach or Unauthorized Release by the Chief Privacy Officer**

The Chief Privacy Officer is authorized to investigate reports of breaches or unauthorized releases of PII by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine, and/or inspect the third-party contractor's facilities and records.

Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer is required to report the breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

Third-party contractors are required to cooperate with the BOCES and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.

Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive this data in violation of applicable laws and regulations, BOCES policy, and/or any binding contractual obligations, the Chief

Privacy Officer is required to notify the third-party contractor of the finding and give the third-party contractor no more than thirty (30) days to submit a written response.

If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law Section 2-d, the Chief Privacy Officer will be authorized to:

a) Order the third-party contractor be precluded from accessing PII from the affected educational agency for a fixed period of up to five years; and/or

b) Order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years; and/or

c) Order that a third-party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data will not be deemed a responsible bidder or offer or on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of General Municipal Law Section 103 or State Finance Law Section 163(10)(c), as applicable, for a fixed period of up to five years; and/or

d) Require the third-party contractor to provide training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to this data and certify that the training has been performed at the contractor's expense. This additional training is required to be performed immediately and include a review of laws, rules, and regulations, including Education Law Section 2-d and its implementing regulations.

e) Determine no penalty be issued to the third-party contractor if the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness, or gross negligence. The Commissioner would then make a final determination as to whether the breach or unauthorized release was inadvertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

Each violation could be punishable by a civil penalty ranging from $1,000 to $10,000.

The Commissioner would then make a final determination as to whether the breach or unauthorized release was inadvertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

**Notification of a Breach or Unauthorized Release**

BOCES will notify affected parents, eligible students, teachers, and/or principals no more than sixty (60) calendar days after the discovery of a breach or unauthorized release of PII by BOCES or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, BOCES will notify parents, eligible students, teachers, and/or principals

within seven (7) calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

a) A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;

b) A description of the types of PII affected;

c) An estimate of the number of records affected;

d) A brief description of the BOCES investigation or plan to investigate; and

e) Contact information for representatives who can assist parents or eligible students that have additional questions.

Notification will be directly provided to the affected parent, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse the BOCES for the full cost of this notification.

**Annual Data Privacy and Security Training**

BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. BOCES may deliver this training using online training tools and this training may be included as part of the training that the BOCES already offers to its workforce.

**Notification of Policy**

BOCES will publish this policy on its website and provide notice of the policy to all its officers and staff.

Education Law § 2-d
8 NYCRR Part 121

Adopted: 6/17/2020
Revised: 01/20/2021
Revised: 9/27/2023