SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

The Board of Trustees ("Board") of the Glens Falls Common School District ("School") is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The Board adopts this policy to implement the requirements of Education Law Section 2-d and Part 121 of the Commissioner's Regulations (hereinafter "implementing regulations"), as well as to align the School's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

a. "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

b) "Building principal" means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c d.

c) "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c d.

d) "Commercial or marketing purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.

e) "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

f) "Disclose" or "disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

g) "Education records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

a)

h) "Educational agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).

i) "Eligible student" means a student who is eighteen years or older.

j) "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States Department of Health and Human Services in guidance issued under 42 USC Section 17932(h)(2).

k) "FERPA" means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

l) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). A copy of the NIST Cybersecurity Framework is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

m) "Parent" means a parent, legal guardian, or person in parental relation to a student.

n) "Personally identifiable information (PII)," as applied to student data, means personally identifiable information as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c(10).

o) "Release" shall have the same meaning as disclosure or disclose under this policy.

p) "Student" means any person attending or seeking to enroll in an educational agency.

q) "Student data" means personally identifiable information from the student records of an educational agency.

r) "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law Sections 3012-c and 3012-d.

s) "Third-party contractor" means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This term will include an educational partnership organization that receives student and/or teacher or principal data from a school district or BOCES to carry out its responsibilities pursuant to Education Law

a)

Section 211-e and is not an educational agency, and a not-for-profit corporation or

other nonprofit organization, other than an educational agency.

t) "Unauthorized disclosure" or "unauthorized release" means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, the School will take steps to minimize its collection, processing, and transmission of PII. Additionally, the School will:

a. Not sell PII nor use or release it for any marketing or commercial purpose or facilitate its use or release by any other party for any marketing or commercial purpose or permit another party to do so.

b) Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and School policy.

c) Ensure that every use and disclosure of personally identifiable information by the School shall benefit its students and the School (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

d) Ensure that personally identifiable information is not included in public reports or other documents.

Except as required by law or in the case of educational enrollment data, the School 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 School.

Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and

principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data and teacher and principal data.

The School will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

The Chief Privacy Officer's powers and duties shall not exceed those provided in Education Law Section 2-d and its implementing regulations.

Data Protection Officer

The School has designated Brian George, Superintendent, to serve as the School's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the School.

The School will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions.

Data Privacy and Security Standards

The School will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

The BOCES will protect the privacy of PII by:

a. Ensuring that every use and disclosure of PII by the School benefits students and the School 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 school operations.

b) Not including PII in public reports or other public documents.

The School affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

Third-Party Contractors

School Responsibilities

The School will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the School, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and School policy.

In addition, the School will ensure that the contract or written agreement includes the third- party contractor's data privacy and security plan that has been accepted by the School.

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

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, consistent with School policy;

b) Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it 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 or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data receive or 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 how it will manage those relationships and contracts to ensure PII is protected;

f) Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the School;

g) Describe whether, how, and when data will be returned to the School, transitioned to a successor contractor, at the School's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and

h) Include a signed copy of the Parents' Bill of Rights for Data Privacy and

Security. Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with the School under which the third-party contractor will receive student data or teacher or principal data from the School, is required to:

a. Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

a)

b) Comply with School policy and Education Law Section 2-d and its implementing regulations;

c) Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);

d) Not use the PII for any purpose not explicitly authorized in its contract;

e) Not disclose any PII to any other party without the prior written consent of the parent or eligible student:

1. Except for 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 School; or

2. Unless 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;

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

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

h) 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.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

Click-Wrap Agreements

Periodically, School 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.

School 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 from the School unless they have received prior approval from the School's Data Privacy Officer or designee.

The School will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap

agreements.

Parents' Bill of Rights for Data Privacy and Security

Pursuant to Part 121 of the Commissioner's Regulations, the School shall create and publish a Parent's Bill of Rights for Data Privacy and Security ("Bill of Rights") to its website. The School will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the School. For each contract the School enters into with a third- party contractor where the third-party contractor receives student data or teacher or principal data from the School, the School will include the necessary supplemental information as required by Part 121 of the Commissioner's Regulations.

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

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

Consistent with the obligations of the School 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 School in a manner prescribed by the School.

The School will ensure that only authorized individuals are able to inspect and review student data. To that end, the School will take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

Requests by a parent or eligible student for access to a student's education records must be directed to the School and not to a third-party contractor. The School may require that requests to inspect and review education records be made in writing.

The School will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the School through its annual FERPA notice. A notice separate from the annual FERPA notice is not required.

The School will comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

The School may provide the records to a parent or eligible student electronically, if the parent consents. The School must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

Complaints of Breach or Unauthorized Release of

Student Data and/or Teacher or Principal Data

The School will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to

the Chief Privacy Officer at NYSED. In addition, the School administration is responsible for developing procedures for parents, eligible students, teachers, principals, and other School staff to file complaints with the School about breaches or unauthorized releases of student data and/or teacher or principal data.

These procedures are provided in the Administrative Regulation to this policy, and will also be disseminated to parents, eligible students, teachers, principals, and other School staff.

The School will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Reporting a Breach or Unauthorized Release

The School will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the School to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the School will be required to promptly notify the School Data Protection Officer of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, School 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 calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the School will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

Notification of a Breach or Unauthorized Release

The School will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the School 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, the School will notify parents, eligible students, teachers, and/or principals within seven 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;
a)

c) An estimate of the number of records affected;

d) A brief description of the School's 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 School for the full cost of this notification.

Annual Data Privacy and Security Training

The School will annually provide data privacy and security awareness training to 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. The School may deliver this training using online training tools.

Notification of Policy

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

Education Law §
2-d 8 NYCRR
Part 121

Adopted: September 17, 2020