CITY SCHOOL DISTRICT OF ALBANY

8635

(X) Required
( ) Local
( ) Notice

INFORMATION AND DATA PRIVACY SECURITY, BREACH, AND NOTIFICATION

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Data Protection Officer is responsible for ensuring the district's systems follow NIST CSF and adopt technologies, safeguards and practices which align with it. This will include an assessment of the district's current cybersecurity state, their target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy district. This appointment will be made at the annual organizational meeting.

The Board directs the Superintendent of Schools, in consultation with appropriate business and technology personnel including the Data Protection Officer to establish regulations which address:

- the protections of "personally identifiable information" ("PII") of student and teachers/principals under Education Law §2-d and Part 121 of the Commissioner of Education;
- the protections of "private information" under State Technology Law §208 and the NY SHIELD Act; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

I. Student and Teacher/Principal "Personally Identifiable Information" under Education Law §2-d

A. General Provisions

PII as applied to student data is as defined in the Family Educational Rights and Privacy Act ("FERPA"), which includes certain types of information that could identify a

student, and is listed in the accompanying regulation 8635-R. PII as applied to teacher and principal data, means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The Data Protection Officer will see that every use and disclosure of PII by the district benefits students and the district (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations). However, PII will not be included in public reports or other documents except where otherwise permitted or required, by Federal or State law or regulations, including, but not limited to, disclosure of directory information permitted under FERPA.

The district will protect the confidentiality of student and teacher/principal PII while stored or transferred using industry standard safeguards and best practices, such as encryption, firewalls, and passwords. The district will monitor its data systems, develop incident response plans, limit access to PII to district employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed or legally required to be maintained.

Under no circumstances will the district sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so. Further, the district will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, to the extent the district maintains any of the following, student data, the district will not report said data to the State Education Department:

1. juvenile delinquency records;
2. criminal records;
3. medical and health records; and
4. student biometric information.

The district has created and adopted a Parent's Bill of Rights for Data Privacy and Security (see Exhibit 8635-E). It has been published on the district's website at http://www.albanyschools.org/files/documents/8635-E_Parent_Bill_of_Rights.pdf and can be requested from the district clerk.

B. Third-party Contractors

The district will ensure that contracts with third-party contractors reflect that confidentiality of any student and/or teacher or principal PII be maintained in accordance with federal and state law and the district's data security and privacy policy.

Each third-party contractor that will receive student data or teacher or principal data must:

1. adopt technologies, safeguards and practices that align with the NIST CSF;

2. comply with the district's data security and privacy policy and applicable laws impacting the district;
3. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):
    a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
    b. unless required by statute or court order and the third-party contractor provides notice of disclosure to the district, unless expressly prohibited.
6. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. use encryption to protect PII in its custody; and
8. not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so. Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the district.

If the third-party contractor has a breach or unauthorized release of PII, it will promptly notify the district in the most expedient way possible without unreasonable delay but no more than seven calendar days after the breach's discovery.

C. Third-Party Contractors' Data Security and Privacy Plan

The district will ensure that contracts with all third-party contractors include the third-party contractor's data security and privacy plan. This plan must be accepted by the district.

At a minimum, each plan will:

1. outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
2. specify the safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;
4. specify how those who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the district;

7. describe if, how and when data will be returned to the district, transitioned to a successor contractor, at the district's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

D. Training

The district will provide annual training on data privacy and security awareness to all employees who have access to student and teacher/principal PII.

E. Reporting

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the district will be promptly reported to the Data Protection Officer, the Superintendent and the Board of Education.

F. Notifications

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the State's Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

The district 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 or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation, or cause further disclosure of PII by disclosing an unfixed security vulnerability, the district 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.

The Superintendent, in consultation with the Data Protection Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

II. "Private Information" under State Technology Law §208

"Private information" is defined in State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for identity theft or permit access to private accounts. "Private

information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the district must be promptly reported to the Superintendent and the Board of Education.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel including the Data Protection Officer, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

III. Employee "Personal Identifying Information" under Labor Law § 203-d

Pursuant to Labor Law §203-d, the district will not communicate employee "personal identifying information" to the general public. This includes:

1. social security number;
2. home address or telephone number;
3. personal email address;
4. Internet identification name or password;
5. parent's surname prior to marriage; and
6. drivers' license number.

In addition, the district will protect employee social security numbers in that such numbers will not be:

1. publicly posted or displayed;
2. visibly printed on any ID badge, card or time card;
3. placed in files with unrestricted access; or
4. used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.

Cross-ref: 1120, District Records
5500, Student Records
8630, Computer Resources and Data Management

Ref: State Technology Law §§201-208
Labor Law §203-d
Education Law §2-d

8 NYCRR Part 121

Adopted: 03-29-12

PARENT BILL OF RIGHTS FOR STUDENT
DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT

Lexia Learning Systems LLC ("Lexia") has been engaged by the City School District of Albany to provide services. In this capacity, the company may collect, process, manage, store or analyze student and/or teacher/principal personally identifiable information (PII).

Lexia Learning Systems LLC will provide the district with licenses to use literacy software-as-a-service.

Lexia Learning Systems LLC ensure that subcontractors or others that the company shares PII with will abide by data protection and security requirements of district policy, and state and federal law and regulations by remaining fully responsible to the District for the actions and obligations of any Lexia service providers or subcontractors (if any), and by including terms and obligations protecting the confidentiality of District PII in its contacts with any such service providers or subcontractors that would access or process District PII. Lexia Learning Systems LLC by entering into an Agreement with the School District acknowledges it has reviewed the relevant District policies on safeguarding PII, including but not limited to, Policy 8635 and Regulation 8635.

PII will be stored securely: Lexia Learning Systems LLC uses Amazon Web Services for its server infrastructure and content delivery. Lexia servers are located in a Tier 1 facility. Physical security and access is provided by a system of access cards, biometric readers, keys, and additional physical controls. A security guard is on duty 24x7. Access to Lexia systems is limited to a subset of Lexia IT personnel, all of whom have undergone background checks. District data is accessed by Lexia employees with a need-to-know, (e.g., customer support, quality assurance, research) to service the customer account, address problems or provide customer-requested support services or improve the customer experience. All Lexia employees undergo a criminal background check annually. All Lexia employees are required to take data privacy training.

If a parent, legal guardian or student contacts us with a request to review the user's Student Records or correct erroneous information, or if an agency, court, law enforcement or other entity contacts us and requests access to Student Records, we will (unless prohibited by writ or compulsory legal process) promptly notify an authorized representative of the applicable Education Client and use reasonable and good faith efforts to assist the Education Client in fulfilling such requests, as required by law and directed by the Education Client.

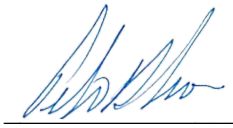
Lexia Learning Systems LLC will take reasonable measures to ensure the confidentiality of PII by implementing the following (*describe the following, as applicable*):

- Password protections
- Administrative procedures
- Encryption while PII is in motion and at rest
- Firewalls, Routers

- Other: employee training

We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, "need-to-know" principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length, and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records.

The contractor's agreement with the district begins on September 1, 2020 and ends on August 31, 2021. Once the contractor has completed its service to the district, records containing student PII will be destroyed or returned within 45 days via the following: Within 45 days following expiration or termination, and as directed in writing by the District account administrator, we start the process of removing and destroying student personally identifiable data in our possession. The designated District account administrator will receive a series of notifications from us following expiration, indicating that student information has been scheduled for removal.



Authorized Representative
Peter Koso, Vice President
Lexia Learning Systems LLC

24-Aug-2020
Date