Policy 8635

(X) Required
(X) Local
(X) Notice

INFORMATION AND DATA PRIVACY SECURITY, BREACH, AND NOTIFICATION

The Board of Education (the "Board") acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. This policy addresses the East Ramapo Central School District's (the "District") 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.

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 overseeing 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 in the District.

Policy 8635

I. Policy Statement

It is the responsibility of District to: (add to here, then capitalize initial word, list below)

1) Comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information;
2) 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) Protect personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure;
4) Address the adherence of its vendors with federal, state and District requirements in its vendor agreements;
5) Train its users to share a measure of responsibility for protecting District's data and data systems;

6) 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) Communicate its required data security and privacy responsibilities and goals and the consequences of non-compliance, to its users.

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

- The protections of "personally identifiable information" ("PII") of students, teachers, and 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.

II. Scope

The policy applies to District employees, and also to users such as independent contractors, interns, student teachers, 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 District. It addresses all information, regardless of the form or format, which is created or used in support of the activities of the District.

This policy shall be published on the District website and notice of its existence shall be provided to all employees and Users.

III. Data Information Privacy and Protection Officers

A. Commissioner of Education Appointed Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer (CPO) 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 District 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, in conjunction with the District's Data Protection Officer.

The Chief Privacy Officer has the power, among others, to:

a) Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by the District that relate to student data or teacher or principal data, which includes, but is not limited to, records related to any technology product or service that will be utilized to store and/or process PII; and,

b) Based upon a review of these records, require the District to act to ensure that PII is protected in accordance with laws and regulations, including but not limited to, requiring the District to perform a privacy impact and security risk assessment.

B. **Data Protection Officer**

The District shall designate a District employee to serve as the District's Data Protection Officer (DPO). The Data Protection Officer for the District shall be the Director of Information Technology Services or other qualified employee of the District as appointed by the Board of Education.

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 District.

The District will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities. Additionally, some aspects of this role may be outsourced to an appropriate District services provider such as a BOCES, to the extent practicable.

The Data Protection Officer shall report to the Superintendent on data privacy 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.

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

A. General Provisions

PII as applied to student data is defined in Family Educational Rights and Privacy Act (FERPA), Policy 5500, which includes certain types of information including but not limited to students records, grades and transcripts that could identify a student, and is listed in the accompanying regulation 8635-R. PII, as applied to teacher and principal data means data which identifies individual teachers and principals, which is confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations such as results of Annual Professional Performance Reviews

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.

The District will protect the confidentiality of student, teacher, and 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.

The District will require that third-party contractors through written form in agreements to return all PII back to the District following the expiration or termination of their agreements (to the extent it can be transferred back, and District requests its return) or it must be physically destroyed. Any PII that cannot be returned, or electronic copies of PII, must be deleted or destroyed. The District will require any contractor to whom it provides PII to provide a certification of secure deletion and/or destruction of PII upon expiration or termination of its agreement with the District no later than ten (10) calendar days after the agreement expires.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in policy and regulation 5500, Student Records.

Under no circumstances will the District sell PII, nor 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, the District will not report the following student 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 https://www.ercsd.org/Page/10342 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; include in contracts 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;
2. Comply with the District's data security and privacy policy and applicable laws, including, but not limited to, Education Law 2-d, 8 NYCRR Part 121, and FERPA, 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. Train those employees who have access to PII in the requirements mandated by federal and state law governing confidentiality of such data prior to receiving access;
5. Not use the PII for any purpose not explicitly authorized in its contract;
6. 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 provide notice of disclosure to the District, unless expressly prohibited.
7. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
8. Use encryption to protect PII in its custody;
9. 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;

10. Return, delete, and/or destroy any PII following the expiration of their agreement or termination of services, and provide certification to the District certifying that action; and,
11. Contact the District immediately in the event of any suspected or actual breach

In the event that a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the District in the most expedient way possible without 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. Acceptable Use Policy, Password Policy and other Related Department Policies

Users must comply with the Acceptable Use Policy in using Department 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 in accordance with State Entity missions and business functions (i.e., least privilege). Accounts will be removed, and access will be denied for all those who have left the agency or moved to another department.

Users must comply with the Computer Resources and Data Management Policy

F. Complaints and Reporting

The District will promptly acknowledge receipt of any complaints, commence an investigation, and take the necessary precautions to protect PII.

Any breach of the District's information storage, digital, 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.

G. Incident Response and Notification

All breaches of data and/or data systems must be reported to the Data Protection Officer. All breaches of 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 District 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. Upon receiving a report of a breach or unauthorized disclosure, the Data Protection Officer and other subject matter experts will determine whether notification of affected individuals is required, and where required, effect notification in the most expedient way possible and without unreasonable delay.

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 ten (10) calendar after such 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 District will be required to promptly notify the District 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, District 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) workdays after the discovery of the breach.

In the event of notification from a third-party contractor, the District will in turn notify the State's Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten (10) workdays after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

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 sixty (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 (7) work 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 and Incident Response Team, 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.

V. "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 that 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, 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.

VI. 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

Adoption date: 06-23-20