INFORMATION AND DATA PRIVACY AND SECURITY BREACH AND NOTIFICATION

The Board of Education acknowledges 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 designates 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.

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" of student and teachers/principal 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. Purpose

This policy addresses Lawrence 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.

II. Policy Statement

It is the responsibility of the District: (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 District's mission; (3) to protect personally identifiable information, and sensitive and confidential information from unauthorized use or disclosure; (4) to address the adherence of its vendors with federal, state and District requirements in its vendor agreements; (5) to train its users to share a measure of responsibility for protecting the District's 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

The District 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

The policy applies to District employees, and also to independent contractors, interns, volunteers ("Users") and third-party contractors who receive or have access to the District's 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 educational agency and it addresses all information, regardless of the form or format, which is created or used in support of the activities of an educational agency

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

V. Compliance

The District is responsible for the compliance of their 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 offices will be directed to adopt corrective practices, as applicable.

VI. Oversight

The District's Data Protection Officer shall annually report to the Lawrence Board of Education 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.

INFORMATION AND DATA PRIVACY AND SECURITY BREACH AND NOTIFICATION

(2) Data protected by law must only be used in accordance with law and regulation and District policies to ensure it is protected from unauthorized use and/or disclosure.

(3) The District 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 personally identifiable information would benefit students and educational agencies, and to ensure that personally identifiable information is not included in public reports or other public documents, or otherwise publicly disclosed;

(4) 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.

(5) The identity of all individuals requesting personally identifiable information, even where they claim to be a parent or eligible student or the data subject, must be authenticated in accordance with District procedures.

(6) It is the District's 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, the District 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.

(7) Contracts with third parties that will receive or have access to personally identifiable information 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.

VIII. Incident Response and Notification

The District will respond to data privacy and security critical incidents in accordance with District policy. All breaches of data and/or data systems must be reported to the Data Protection Officer/Chief Information 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.

State and federal laws require that affected individuals must be notified when there has been a breach or unauthorized disclosure of personally identifiable information. Upon receiving a report of a breach or unauthorized disclosure, the Superintendent, Data Protection Officer, Counsel 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.

IX. Acceptable Use Policy, Password Policy and other Related Department Policies

(1) Users must comply with the Acceptable Use Policy in using District 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 District 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. (2) Users must comply with the Password Policy. (3) All remote connections must be made through managed points-of-entry in accordance with District Policies.

X. Training

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

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

Adoption date: June 13, 2011
Revised: November 2020
Revised Policy Adopted by BOE: March 8, 2021

INFORMATION AND DATA PRIVACY AND SECURITY BREACH AND NOTIFICATION REGULATION

Definitions

"Private information" shall mean personal information (i.e., information such as name, number, symbol, mark or other identifier which can be used to identify a person) in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- Social security number;
- Driver's license number or non-driver identification card number; or
- Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

Note: "Private information" does not include publicly available information that is lawfully made available to the general public pursuant to state or federal law or regulation.

"Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district. Good faith acquisition of personal information by an officer or employee or agent of the district for the purposes of the district is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

To successfully implement this policy, the district shall inventory its computer programs and electronic files to determine the types of personal, private information that is maintained or used by the district, and review the safeguards in effect to secure and protect that information.

Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the district shall consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded or copied;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts, opened or instances of identity theft reported; and/or
4. any other factors which the district shall deem appropriate and relevant to such determination.

INFORMATION AND DATA PRIVACY AND SECURITY BREACH AND NOTIFICATION REGULATION

Security Breaches – Procedures and Methods for Notification

Once it has been determined that a security breach has occurred, the following steps shall be taken:

1. If the breach involved computerized data *owned or licensed* by the district, the district shall notify those New York State residents whose private information was, or is reasonably believed to have been acquired by a person without valid authorization. The disclosure to affected individuals shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system.
   The district shall consult with the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures.
2. If the breach involved computer data *maintained* by the district, the district shall notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been acquired by a person without valid authorization.

Note: The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after the law enforcement agency determines that such notification does not compromise the investigation.

The required notice shall include (a) district contact information, (b) a description of the categories information that were or are reasonably believed to have been acquired without authorization and (c) which specific elements of personal or private information were or are reasonably believed to have been acquired. This notice shall be directly provided to the affected individuals by either:

1. Written notice
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the district keeps a log of each such electronic notification. In no case, however, shall the district require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.
3. Telephone notification, provided that the district keeps a log of each such telephone notification.

However, if the district can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds

INFORMATION AND DATA PRIVACY AND SECURITY BREACH AND NOTIFICATION REGULATION

500,000; or (c) that the district does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when the district has such address for the affected individual;
2. Conspicuous posting on the district's website, if they maintain one; and
3. Notification to major media

Notification of State and Other Agencies

Once notice has been made to affected New York State residents, the district shall notify the State Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the district shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

1st Presentation: November 16, 2010
2nd Presentation: February 15, 2011
3rd Presentation: June 13, 2011

Adoption date: June 13, 2011
Revision date: March 8, 2021