EAST STROUDSBURG AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: INFORMATION PROTECTION

ADOPTED: NEW POLICY

REVISED:

830. INFORMATION PROTECTION POLICY

1. Purpose

The East Stroudsburg Area School District ("School District") recognizes the advances in technology, communications, data and information storage, and transmission have afforded the School District vast benefits. They have also generated risks to privacy and security of information that the School District gathers, uses, and holds to perform its educational mission and business responsibilities. Personal identities, privacy, confidential information, communications, and other information are vulnerable to unauthorized disclosures, breaches, loss, or theft. The responsibility to protect such information is complex, intricate, challenging, and necessary. 24 P.S. § 5-510

Through this policy, relevant administrative regulations and other requirements the School District is providing guidance in protecting its private and confidential information. The School District will periodically reassess risks and update this policy, and other accompanying and relevant policies, regulations, procedures, standards, rules, as well as its practices.

2. Definitions

Confidential Information includes information that can harm the School District or its employees, students, or others if it is improperly disclosed.

Confidential information is information for which unauthorized disclosure or unauthorized modification would result in significant loss to the School District, impair its ability to conduct its educational mission and business, or result in a violation of various rights of students, employees, and others, and federal or state laws or regulations.

Examples include: Contractual agreements, intellectual property rights, safety or physical security of a building, public utility, resource, infrastructure, facility, information security system, and technology and computer security systems.

Federal or state laws or regulations, include, but are not limited to:

1. Family Educational Rights and Privacy Act ("FERPA"). 20 U.S.C. § 1232(g), 34 C.F.R. § 99.1 et seq.

2. Children's Online Privacy Protection Act ("COPPA"). 15 U.S.C. §§ 6501 et seq., 16 C.F.R. 312.1 et seq.

3. Individuals with Disabilities Education Act ("IDEA"). 20 U.S.C. §§ 1400 et seq.; 34 C.F.R. Parts 300 – 301.

4. Children's Internet Protection Act ("CIPA"). 47 U.S.C. § 254(h)(5).

5. The Strengthening Career and Technical Education for the 21st Century Act, reauthorized and amended in 2018 ("Perkins V"). 20 U.S.C. § 2301 et seq.

6. Health Insurance Portability and Accountability Act ("HIPAA")[. Public Law 104-191.

7. Health Information Technology for Economic and Clinical Health ("HITECH Act"). 42 U.S.C. §§ 300jj et seq.; §§ 1790 et seq.

8. Pennsylvania Right-to-Know Law ("RTKL"). 65 P.S. 67.101 et seq.

Confidential Information also includes Personally Identifiable Information (PII) and Sensitive Information (SI).

Examples: PII, SI, and other confidential information, such as but not limited to, student data that is not considered directory information, and information that is protected by a non-disclosure agreement.

Personally Identifiable Information (PII) is defined differently in different laws. School District officials, employees, students, board members, and Guests[1] must be cognizant of the applicable definition of PII and adhere to the applicable legal basis for the data and information they use. Examples include:

COPPA - When the issue involves the COPPA, PII means individually identifiable information about an individual collected online, such as:

1. First and last name;

2. Home or other physical address including street name and name of a city or town;

3. Online contact information;

4. Screen or user name where it functions in the same manner as online contact information;

5. Telephone number;

5. Social Security number;

6. Persistent identifier that can be used to recognize a user over time and across different websites or online services. Persistent identifier includes, but is not limited to:

   - Customer number held in a cookie;
   - Internet Protocol (IP) address:
   - Processor or device serial number, or unique device identifier:
   - Photograph, video, or audio file where such file contains a child's image or voice;
   - Geolocation information sufficient to identify street name and name of a city or town; or
   - Information concerning the child or the parent(s)of that child that the operator collects online from the child and combines with an identifier described in this definition. 15 U.S.C. §§ 6501 et seq., 16 C.F.R. 312.1 et seq.; 73 P.S. § 2301.

Pennsylvania's Breach of Personal Notification Act - If Pennsylvania's Breach of Personal Information Notification Act is at issue, PII includes: an individual's first name or first initial and

[1] As defined in the School District's Acceptable Use Policy 815, "Guests include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff and students, board members, independent contractors, and School District consultants and vendors." Pol. 815.

last name in combination with and linked to any one or more of the following, when not encrypted or redacted:

1. Social Security number;

2. Driver's license number or a State identification card number issued in lieu of a driver's license;

3. Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. 73 P.S. § 2301.

FERPA - If FERPA is at issue, PII includes, but is not limited to:

1. Student's name;

2. Name of the student's parent or other family members;

3. Address of the student or student's family;

4. Personal identifier, such as the student's Social Security number, student number, or biometric record;

5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

   Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. 20 U.S.C. § 1232(g), 34 C.F.R. § 99.1 et seq. See also: 22 Pa. Code § 12.31 - § 12.32

HIPAA - If HIPAA is at issue, protected health information (PHI) includes the definitions of "health information" and "individually identifiable health information" in HIPAA, and "protected health information" in the HITECH Act, except PHI may exclude (1) specifically listed "individually identifiable health information," and (2) "PHI" that meet the de-identified standard and implementation specifications. Public Law 104-191; 42 U.S.C. §§ 300jj et seq.; §§ 1790 et seq.

Sensitive Information (SI) is information for which unauthorized disclosure or unauthorized modification may or may not result in a direct legal, contractual, regulatory, or other violation. SI is generally intended for use within the School District or within a specific, department or group of individuals with a legitimate need-to-know the sensitive information.

Examples: personal cell phone numbers, internal memos, incomplete or unpublished notes of teachers or psychologists, ongoing or active investigation information, information pertaining to active litigation, employee documents such as evaluations, corrective action plans, disciplinary actions, and termination documentation, student psychological, medical, and psychiatric reports, and board of school director executive session documents. [18]

	Public Information (PI) is School District information that has been explicitly approved for distribution to the public or through some other valid authority, or complies with Pennsylvania's Right-to-Know Law. Examples: School District brochures providing information about the School District services, directory information, press releases. **Users** include students, employees, board members, Guests, vendors, and others who are using the School District's CIS systems[2] and cloud computing services.
3. Authority	The School District shall take measures to strictly protect its CIS Systems against outside and internal risks and vulnerabilities. Users are important and critical to protecting these School District assets and in lessening the risks that can destroy them. Consequently, the Board establishes that the School District's CIS Systems must be used in compliance with this Policy, other School District policies, regulations, rules and procedures; Internet service providers, and cloud, fog, and mist providers; website, and App terms (if they are lawful); and local, state and federal laws and procedures. Users are required to fully comply and must immediately report any violations or suspicious activities to the Superintendent, and/or designee(s) who shall report any violations to the Superintendent. Failure to report shall result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section found at the end of this Policy, and provided in other School District policies, agreements, and local, state and federal regulations and laws. 24 P.S. § 5-510; Pol.815. CIS systems include: 1. School District computers which are located or installed on School District property, at School District events, connected to the School District's network or systems, or when using its mobile commuting equipment, telecommunication facilities in protected and unprotected areas or environments, directly from home, or indirectly through another provider; and/or 2. When Users bring and use their own personal computers and devices, and 3. When Users bring and use another entity's computers or devices to a School District location, event, or connect it to the School District network(s) or system(s). Access to the School District's CIS Systems through its resources is a privilege, not a right. The CIS Systems, as well as the User accounts and information are the property of the School District. The School District, further, reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The School District will cooperate with other educational entities, providers, appropriate authorities, and local, state, and federal officials to the extent legally required in any investigation related to the misuse of the CIS Systems, whether criminal or civil. Pol. 815.

[2] CIS systems is defined in the School District's Acceptable Use Policy as "Computers, networks, Internet, Electronic Communications, information systems, databases, files, software, and media." Pol. 815.

4. Delegation of Responsibility	The Superintendent, and/or designee(s), is/are granted the authority to create, update, and enforce additional administrative regulations, procedures, and rules to carry out the purpose of this Policy. The administrative regulation(s), procedures, and rules accompanying this Policy must include the National Institute of Standards in Technology ("NIST") Cybersecurity Framework ("CSF"), which include guidance in Identifying, Protecting, Detecting, Responding and Recovery relevant to cybersecurity concerns. The guidance functions are supported by categories, sub-categories, and information references. NIST CSF (U.S. Department of Commerce); nist.gov. **Identify Functions** Identify functions require the School District to develop an organizational understanding to manage cybersecurity risks to systems, people, assets, data, and capabilities. Activities in the Identify Function are foundational for effective use of the CSF Framework. Understanding the business and educational context, the resources that support critical functions, and the related cybersecurity risks enables the School District to focus and prioritize its efforts, consistent with its risk management strategy and business and educational needs. Examples of outcome categories within the Identify Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy. **Protect Functions** Protect functions require the School District to develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within the Protect Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology. **Detect Functions** Detect Functions require the School District to develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome categories within the Detect Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes. **Respond Functions** Respond Functions require the School District to develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

	The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome categories within the Respond Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements. **Recover Functions** Recover Functions require the School District to develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome categories within the Recover Function include: Recovery Planning; Improvements; and Communications. The Superintendent, and/or designee(s) must form an Information Risk Management Team that: (1) meets periodically, (2) that operates under School District Administrative Regulations, Procedures, and Rules, and (3) that is accountable for ensuring that policies, processes, and internal controls are implemented and operating to prevent and address data and information risks. The Team must establish a School District Cyber Security Team to execute the responsibilities essential to assisting with the NIST CSF Functions.
5. Guidelines	**<u>Guidelines: Protecting Confidential Information</u>** **Information Protection Procedures** The Information Risk Management Team and Cyber Security Team are required to create School District Procedures based on the NIST CSF's Identify, Protect, Detect, Respond and Recovery Framework. The Procedures must apply to the NIST CSF's categories and sub-categories functions that are determined by the Teams to apply to the School District. The purposes of the Procedures are to assist in implementing and operating processes and internal controls to prevent and address data and information risks. NIST CSF (U.S. Department of Commerce); nist.gov. **Records Retention and Destruction** Confidential Information must be retained in accordance with the School District's Records Retention and Destruction Policy and Records Retention and Destruction Schedule.[23] Physical and electronic copies of Confidential Information must be securely destroyed pursuant to methods, technology standards, technology infrastructure, statutes, regulations, and agreements, requirements for specific information, and the School District's Records Retention and Destruction Policy and Records Retention and Destruction Schedule. Records Retention and Destruction Policy and Schedule, Pol. 800.

Data Disclosure, Breach, Loss or Theft

Security breaches can come from many sources, internal or external, and can occur at any time. The cause may be intentional, negligent, or even from a hardware malfunction. Once a breach occurs, the damage may spread and multiply with incredible speed. To minimize the likelihood of any breach and to mitigate its consequences, employees, students, Guests, board members, and third parties must be vigilant. Careful real-time monitoring of practices can help ensure compliance with the privacy and security policies and better safeguard information both within the School District and in the hands of any employee, student, Guest, board member, or third party.

If an unauthorized disclosure, breach, loss, or theft of private and/or confidential information occurs, employees, students, Guests, board members, and third parties must comply with the School District's Data Breach Notification Policy and Incident Response Procedures.

A potential breach must be reported as soon as possible to the Information Risk Management Team and Cyber Security Team. The Teams shall follow the Incident Response procedure guidelines. 73 P.S. § 2301.

Employees

All employees, Guests, students, board members and other individuals are responsible for understanding the confidentiality and sensitivity of information they encounter during the course of their responsibilities, and for protecting the information as described in this Policy, and any regulation, procedure, or rule.

Employees, Guests, students, board members, and other individuals who require access to Confidential Information to carry out their School District responsibilities must be trained about this Policy and other relevant School District policies, regulations, rules, and procedures.

Training must be provided to all Users. The training must include, among other issues, the identification of data and information categories and the protection relevant to each one, the identification and explanation about applicable state and federal laws, and the identification and explanation relevant to the nature of the data and information privacy and security issues and the employees' obligations applicable to them.

In addition to training that is required for all employees, students, Guests, board members, and other individuals relevant to Confidential Information, the IT employees, and other individuals who are required to access PII and SI to carry out their responsibilities and to update the School District cybersecurity standards, NIST Functions, categories, and sub-categories must be trained, as appropriate and relevant. The training must include: (1) information privacy and security standards, and controls; (2) relevant state and federal statutes and regulations; (3) technology security and privacy standards and controls; (4) and other best practices as they rapidly evolve.

PII shall only be collected when it serves a specific purpose, and only the minimum amount of PII shall be collected to serve the specific purpose.

Employees shall not use Confidential Information for any purpose other than completing School District job functions.

Protecting PII and SI requires all the protections of Confidential Information.

	Any changes to the information systems that store Confidential Information must follow the School District's approved procedures. The Superintendent, and/or designee(s), must maintain an inventory of all PII and SI, and shall be responsible to oversee the protection of each set of PII and SI. **Exceptions** Any exceptions to this Policy must be approved and recorded by the Information Risk Management Team, presented to the School District's Administrative Team, and when appropriate, presented to the Board of School Directors for ratification or approval. **Consequences for Inappropriate, Unauthorized and Illegal Use** Disciplinary consequences shall be in accordance with this Policy and other relevant School District policies, regulations, rules, and procedures, including but not limited to Student Discipline (Pol. 218), Conduct/Disciplinary Procedures (Pol. 317), Acceptable Use (Pol. 815), and other relevant policies, regulations, procedures, and local, state, and federal law. Violations of this Policy must be reported to the Superintendent, and/or designee(s).