No. ~~816.2~~830.1

2022 DRAFT

SECTION: EMPLOYEES AND GUESTS

TITLE: PRIVACY AND SECURITY OF STUDENT ELECTRONIC AND DIGITAL INFORMATION

EAST STROUDSBURG AREA SCHOOL DISTRICT

ADOPTED: December 15, 2014

REVISED: _____, 2022

~~816.2~~830.1 PRIVACY AND SECURITY OF STUDENT ELECTRONIC AND DIGITAL INFORMATION

1. Purpose

The privacy and security of some student information is protected from unauthorized access, transfer, transmission, disclosure, and storage by numerous laws. ~~For example, the Family Education Rights and Privacy Act ("FERPA"), Children's Online Privacy Protection Act ("COPPA"), Individuals with Disabilities in Education Act (2004) ("IDEA 2004"), and if relevant other laws such as the Health Insurance Portability and Protection Act ("HIPAA"), the Health Information Technology Act ("HITECH Act"), and the Carl D. Perkins Act Vocational and Technical Education Act ("Perkins").~~ The School District governs student data and information protection through ~~these and other~~ federal, state and local privacy and security laws and regulations, technology standards, and School District policies, regulations, rules, procedures, and practices.

The School District has adopted this Policy to minimize access to sensitive, confidential, and personally identifiable information within the School District and outside of the School District through a variety of controls and disclosure avoidance methods, and best practices.

Student information is a vital component of the School District's operations, and it is important to ensure that persons with a need for student data and information have ready access to that data and information. It is equally important to ensure that measures have been taken to protect critical information against accidental, voluntary, or unauthorized access, transfer, transmission, disclosure, storage, modification, or destruction, in order to ensure the security, reliability, integrity and availability of the internal and external use of student information, and to lessen the collection, mining, profiling, and external use of student information.

The steady proliferation of technologies that allow, and business models that depend on, the collection and monetization of students' and children's information and data through sophisticated practices raise concerns that call for strengthening students' privacy protections.

Employees and Guests must be diligent in protecting student data and information in mobile devices, cloud-based services, computers, printers, systems, and other electronic and digital devices, equipment, locations, systems, services, and activities.

	They must also be diligent in protecting student information and data from the targeting practices of providers of educational technology tools, as well as other online providers that students, employees, and parents use for their education and school-related activities.~~, and through Data Minimalization.~~ Underappreciated risks and often ignored data and information security and privacy precautions and procedures are harmful to students, the School District, and to others.
2. Definitions National Center of Education Statistics (NCES) Technical Brief #2 "Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records" (NCES 2011-602).	**Data Minimization:** Data Minimization is the practice of only collecting School District Student Data and Information that is directly relevant and necessary to accomplish specified purpose(s) and complies with the School District's Plan for the Collection, Maintenance, and Dissemination of Student Records, and for only retaining School District student Data and Information for as long as is necessary to fulfill the specified purpose(s) and School District's Records Retention and Records Destruction Policy and Schedule requirements. It also extends to only allowing access to specific School District Student Data and Information elements to those individuals who have an authorized and a legitimate need to view and utilize those elements. **Guests:** Guests include, but are not limited to, volunteers, adult education staff and students, board members, independent contractors, and School District consultants who are authorized by the School District to have access to School District Student Data and Information. **School District Student Data and Information:** School District Student Data and Information is defined as all information content related to the students of the School District that exists in electronic, digital or paper form. The degree of protection required for different types of Student School District Data and Information is based on the nature of the data and information compliance requirements. The following four classification levels will be used for classifying School District Student Data and Information: • **Confidential Data:** Confidential Data is School District Data 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 contractual agreements or federal, ~~or~~ state, or local laws or regulations, technology standards, School District policies, regulations, rules, procedures, and practices ~~including, but not limited to FERPA, COPPA, IDEA (2004), CIPA, Perkins, HIPAA, and HITECH Act~~. *Examples: Social Security Numbers, medical records, student data that is not considered directory information, information protected by a non-disclosure agreement.* • **Personally Identifiable Information:** Personally Identifiable Information is defined differently in different laws. School District officials, employees, and Guests must be cognizant of and adhere to the applicable legal basis for the

	student data and information they are dealing with and apply the applicable definition of personally identifiable information. *Example*s*: When the issue involves the COPPA law, personally identifiable information includes: geolocation data, photos, videos, and audio files that contain a child's image or voice, and persistent identifiers (tracked cookies). If the Pennsylvania's Breach of Personal Information Notification Act is at issue, personally identifiable information includes: an individual's first name or first initial and last name in combination with and linked to any one or more of the following, when not encrypted or redacted: Social Security number; driver's license number or a State identification card number issued in lieu of a driver's license; 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.* • **Public Data**: Public Data is School District Data 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.* • **Sensitive Data**: Sensitive Data is School District Data for which unauthorized disclosure or unauthorized modification would not result in direct legal, contractual or regulatory violations, but may otherwise adversely impact the School District students. Sensitive Data is generally intended for use within the School District or within a specific unit, department or group of individuals with a legitimate need-to-know. *Examples: personal cell phone numbers, internal memos, incomplete or unpublished notes of teachers or psychologists.*
3. Authority	The School District's polic<u>i</u>es, administrative regulations, rules, procedures, and practices must be complied with and are incorporated into this Policy, including but not limited to the Student Records Policy, the Plan for the Collection, Maintenance and Dissemination of Student Records; the School District's HIPAA Plan; the Social Media Policy and its accompanying Administrative Regulations; the Acceptable Use Policy and its accompanying Administrative Regulation (if any); the Student Electronic Communication Device Policy; the Data Breach Notification Policy; the Cloud Computing Policy; and the student, employee, and Guest disciplinary policies, regulations, rules, procedures, and practices. The Superintendent is granted the authority to create and enforce an administrative regulation to accompany this Policy, at his/her discretion. This Policy must be incorporated into the accompanying administrative regulation, if it is created.

4. Delegation of Responsibility	The Records Management Coordinator is responsible for addressing employee and Guest questions, conduct, and disciplinary issues pertaining to the privacy and security of student data and information. The Records Management Coordinator is responsible for protecting the privacy and security of student data and information. The Superintendent, and/or designee(s), is responsible for developing security procedures and guidelines pursuant to this Policy, ensuring that such procedures and guidelines are published and distributed to all employees and relevant Guests, and conducting periodic reviews of such procedures and guidelines. The developed procedures and guidelines will serve as the standards of information and data security to be applied by employees, including technology and information employees, and information users, such as teachers, aides, and volunteers, and they will be the basis for compliance monitoring, review and audit. The School District staff will ensure that the standards for data and information privacy and security that affect their respective areas of responsibility are effectively implemented. The administrative duties associated with this responsibility will be assigned by the Superintendent and Records Management Coordinator to designated employees, who typically are the managers responsible for the creation or collection of specified School District Student Data and Information.
5. Guidelines ESASD Cloud Computing Policy	*Cloud Computing, Storage and Services* 1. Different kinds of cloud computing, storage, and/or services could be used by the School District (for example: a public cloud, a private cloud, a community cloud, a hybrid cloud, or a partner cloud) for different types of cloud computing, storage, and/or services (for example: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)). However, some providers may offer and deliver more than one kind or type of service. Employees and Guests must only use School District authorized kinds and types of cloud computing, storage, and services for School District Student Data and Information. 2. Many products and services that can be used in School Districts are run in clouds provided by third party service providers as opposed to on the servers operated by the School District. The third party operation, control, and storage can raise data protection, privacy, and security issues, and violate laws applicable to the School District. Products and services are available with or without monetary payment for employees and Guests to deploy directly in their classrooms or with students. However, a formal School District process must be used by employees and Guests, where compliance and other issues are evaluated, for their use of cloud services to be authorized by the School District.

	2.1. Employees and Guests may not place, transfer, transmit, and store School District Student Confidential, Sensitive, and Personally Identifiable Data and/or Information in cloud products and/or services without the consent of the School District. As an example, teachers working on a student's IEP and storing it in their personal cloud service account such as DropBox, is not authorized by the School District. 2.2. School District Student Confidential, Sensitive, and Personally Identifiable Data and Information may be required to be encrypted with School District authorized encryption during use. If so, employees and Guests must use the authorized encryption and, if appropriate, decryption software/service. Use of unauthorized encryption, decryption, and anonymizers are prohibited. 2.3. Employees and Guests must be notified that it is possible for School District Student Confidential, Sensitive, and Personally Identifiable Data and Information to be accessed, transferred, transmitted, disclosed, and stored in the cloud when using mobile devices, as well as desktop computers, from any location. The privacy and security of Student Confidential, Sensitive, and Personally Identifiable Data and information must be protected. 2.4 Google Workspace~~Apps~~ for Education (GW~~A~~FE) is a cloud service. Employees and Guests must not use GW~~A~~FE for School District Student Confidential, Sensitive, and Personally Identifiable Data and Information until or unless privacy and security protections are certified and approved. 2.5 Only authorized School District administrators using authorized School District procedures may enter into cloud computing, cloud services, and/or cloud storage contracts. Other employees, Guests, and students may not agree to contractual terms that subject the School District to cloud agreements, terms, and conditions. For example, a teacher may not click and "agree" to download an App for instructional material to use with students without School District approval.
34 C.F.R. §99.33	2.6 The School District must set up reasonable methods to ensure employees and Guests access only student records in which they have a legitimate educational interest (physical, technological, and administrative controls to prevent unauthorized use). 2.7 The School District may not give cloud providers student Confidential, Sensitive, and Personally Identifiable Data and Information solely for the provider's commercial behavioral advertising and student user profile product development and marketing. *Online Application Software (Apps)* 1. School District officials must establish rules and procedures to comply with

	the COPPA restriction on sharing School District students' personally identifiable information (geolocation data, photos, videos, and audio files that contain a child's image or voice, and persistent identifiers (tracked cookies)) in mobile Apps, and third-party web sites plugins, web sites, and some online services without parent verifiable consent. 2. The School District may act as the agent of a parent(s) to provide consent for the collection of student personally identifiable information if certain notifications and procedures required by COPPA are put into place. 3. The School District may not authorize the commercial collection of School District Student Confidential, Sensitive, and Personally Identifiable Data and Information be collected, used, and/or shared for behavioral advertising or building a student user profile. However, the School District may contract for the sole purpose and benefit of the School District's use of the students' data and information (for example, a gradebook). 4. Only authorized School District administrators using authorized School District procedures may enter into App contracts for the use with or by School District employees and students. Employees, Guests, and students may not agree to contractual terms that subject the School District to agreements, contracts, terms and conditions. For example, a teacher may not click and "agree" to download an App for instructional material to use with students without School District approval. 5. Contracts must comply with legal requirements, and consider the needs of the School District. Some essential issues include: (1) data security, privacy and confidentiality, (2) School District access to and location of data and information, (3) service levels and remedies, (4) limitations and liabilities, disclaimers of warranties, (5) pricing, (6) jurisdiction, and (7) suspension and termination of service rights. *Targeting Practices and Automated-Decision Making (AI)* Sophisticated targeting practices of providers comprehensively collect students' activities, information, and data across the Internet, then use, sell and/or share them with third parties, including for marketing purposes and automated decision-making. In addition to Apps, students, employees, and parents need to examine the use of automated decision-making technology (artificial intelligence). Automated decision-making could be beneficial or detrimental. For example. it may be beneficial through the use for students' adaptive learning software, virtual assistants, and what videos to watch or music to listen to, but it could be detrimental if the data set is biased, the algorithm is exaggerated, and/or the use of the automated decision-making is not trustworthy. Providers should be able to explain, be transparent and be truthful about their tools for the school, employees, and students to understand and use them. Employees should request information about the automated decision-making of the
Section 5 of the Federal Trade Commission Act	
National Institute of Standards and Technology (NIST)	

	tools when contracting with a provider and when deciding on the use of online sources. *Inappropriate Disclosure* If a School District employee or Guest discovers that School District Student Confidential, Sensitive, and Personally Identifiable Data and/or Information has been disclosed inappropriately, and the students whose data and/or information were disclosed are put at risk of identity theft or other harm, the employee must immediately notify the Records Management Coordinator, who will work with the attorney to ensure that those parents or students are notified promptly, and comply with the School District's Data Breach Notification Policy. *Training*
20 U.S.C. § 1232g, 34 C.F.R. Part 99.1 et seq.	All employees and Guests who use School District Student Data and Information must receive training about the privacy and security of student information. Included in the training must be information about (1) how to protect the privacy and security of student data and information of employees' and Guests' personal and School District mobile devices as well as desktop computers; (2) how to incorporate Data Minimization into the use of student information; (3~~2~~) how the secondary use of student information by third parties functions, such as App developers, marketers, cloud services, web sites, data mining services, and automated decision-making providers, (4~~3~~) the legal and regulatory requirements to protect student information and data; (5~~4~~) the technological ways student data and information may be acquired; and (6~~5~~) how to determine whether and what private data and information an App, web site, cloud service, or other data or information service collects and what they do with the data and information. *Consequences for Violation(s) of School District Policy*
ESASD Policies	A founded charge against a School District employee or Guest who violates this Policy may subject such employee or Guest to disciplinary action, up to and including discharge. Appropriate consequences and remedial actions range from positive behavioral interventions to and including suspension or dismissal, and may include counseling, employee or Guest conferences with supervisors and/or administrators, warnings, usage restrictions, loss of School District privileges, reassignment, oral or written reprimands, and/or legal proceedings. Any violation of this Policy shall be considered an infraction of the Policy and alsdo may be considered a violation(s) of other applicable School District policies, with discipline implemented accordingly on a case-by-case basis. Any violation of the Pennsylvania Crimes Code will be reported to law enforcement.

	References: • Pennsylvania School Code – 24 P.S. §5-510 • State Board of Education Regulation – 22 Pa. Code §12.3 • *Carl D. Perkins Act Vocational and Technical Education Act ("Perkins")* – 20 U.S.C. § 2301 et seq. • *Children's Internet Protection Act ("CIPA")* - 47 U.S.C. §254(h)(5)(B)(iii) • *Children's Online Privacy Protection Act ("COPPA")* – 16 U.S.C. §§ 6501 et seq., 16 C.F.R. 312.1 et seq. • *Family Educational Rights and Privacy Act ("FERPA")* – 20 U.S.C. § 1232g, 34 C.F.R. Part 99.1 et seq. •. Federal Trade Commission Act, § 5 • *Health Insurance Portability and Accountability Act ("HIPAA")* – 42 U.S.C. § 300gg, 29 U.S.C. § 1181, 42 U.S.C. § 1320d et seq.; 45 C.F.R. §§ 144, 146, 160, 162, 164. • *Health Information Technology for Economic and Clinical Health Act ("HITECH Act" or "Health Information Technology Act")* - 45 C.F.R. Part 160 and 164 • *Individuals with Disabilities Education Act (2004) ("IDEA 2004")* – 20 U.S.C. §§ 1400 et seq.; 34 C.F.R. Parts 300 – 301. • ESASD Board Policies, Administrative Regulations, Rules, and Procedures •. National Institute of Standard and Technology (NIST) • The *ESASD Student Records Plan for the Collection, Maintenance, and Dissemination of Student Records* • The *ESASD HIPAA Plan* • The *ESASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws*