Technology usage has become more ubiquitous. School districts are confronted with its Users keeping student, employee, and School District confidential, personally identifiable, sensitive, and proprietary data and information with undisclosed unauthorized parties and located in many unprotected and unknown locations. At the same time, cloud services technology has evolved to provide a large number and a variety of services and opportunities that are useful to the educational programs at the Chambersburg Area School District (“School District”). The purpose of this regulation is to centralize how the School District’s information and data are stored and used in order to maximize instructional utility for all Users, while at the same time maintaining the School District’s and other legally mandated levels of data and information confidentiality and protection.

Definitions

Cloud Computing - Cloud computing is a general name for what is actually several types of computer infrastructures. It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Generally, five essential characteristics, three service models, and five deployment models of cloud computing currently exist.\(^1\)

Users – Users include students, employees, guests,\(^2\) vendors, and other who are using the School District’s CIS systems\(^3\) and cloud computing services.

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

\(^1\) The five “essential characteristics” are (i) on-demand self-service, (ii) broad network access, (iii) resource pooling, (iv) rapid elasticity, and (v) measured service. The three “service models” are (i) Software as a Service (SaaS)(capability for the School District to use the provider’s applications running on a cloud interface that is usually accessed through a web browser, but the School District does not have control over the cloud infrastructure or underlying hardware), (ii) Platform as a Service (PaaS)(provider-given programming languages allow the School District to develop and run its own applications, to have control over its applications and application environment but the School District does not control the underlying cloud hardware), and (iii) Infrastructure as a Service (IaaS)(the School District is able to provision computer hardware in order to run arbitrary software, including operating systems and applications, and has control over hardware, storage, and applications, but the School District does not manage the cloud infrastructure). Some providers may include more than one type of service. The five “deployment models” include (i) the private cloud, (ii) the community cloud, (iii) the public cloud, (iv) partner cloud; and (v) the hybrid cloud.

\(^2\) As defined in the School District’s Acceptable Use Policy, “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.”

\(^3\) 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.”
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 laws or regulations, 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.

  Examples: 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.

**Delegation of Authority**

The superintendent must work in conjunction with the principals and Information Technology Department (IT) to create and implement an effective cloud computing system for educational use
and storage of data and information. The superintendent may delegate responsibilities if clear guidance is provided to those with the delegated responsibility while (s)he maintains the ultimate authority to enforce this regulation.

Users must be notified about, trained, and consent to the appropriate use of cloud computing. Users who use the School District’s CIS systems, and information and data must comply with the School District’s CIS systems security requirements, including the School District’s Acceptable Use Policy, Data Breach Notification Policy, other relevant School District policies, regulations, rules and procedures, website and ISP terms, and local, state and federal laws and procedures.

**Regulations**

1. Users must keep all School District (including but not limited to personally identifiable, confidential, and sensitive employee and student) information and data in the School District’s and in its contracted parties’ CIS systems, and storage, unless an exception is permitted and granted in writing by the Superintendent, and/or designee, or Users are permitted by an exception in a School District policy, regulation, rule, or procedure. This means that Users must not place or keep School District information and data in a cloud computing service, or virtual or online storage, beyond the control, access, protection, and safety of the School District, unless written permission is granted to the specific individual by the Superintendent, and/or designee, or it is approved through School District policy, regulation, rule or procedure. Users must agree to protect the privacy and security of School District information and data.

2. Anonymity of Users’ activities to the provider must be a central aspect of protecting Users’ privacy, much of the information flowing through the cloud will not only have to be protected in terms of who it belongs to, but also what it is. A variety of data encryption, security, and availability is being used by the School District. Therefore, Users must not circumvent the encryption and other data security protections and they must fulfill their responsibilities to protect against associated privacy and security risks, such as using strong passwords, protecting their passwords, and not sharing their passwords with others. See the School District’s Acceptable Use Policy and Vendor Access Policy for additional guidance.

3. Technical assistance issues, privacy and security problems, and vulnerabilities (such as but not limited to hacking and other data integrity issues) of the cloud services must be reported immediately to the Director of Technology, or designee.

4. Access to data and information must be tiered within the cloud to those who have authorization. For example: administrators may have access to the students’ and teachers’ data and information in their school, but not to all students and teachers in the School District. The tiered access and/or authorization may be modified as services are expanded or narrowed by the administration.

5. Parental access to student records may be allowed by the use of guest passwords with specifically tailored access.

6. All content that Users post in School District utilized cloud computing services must comply with copyright laws, and the School District’s Acceptable Use and Copyright policies. Users must set pages to reflect whether they want to share their work or whether they want to protect their copyrighted work.
7. Users must not post, possess, store, process, or transfer unlawful, threatening, libelous, defamatory, pornographic, obscene, harassing, or other content that violates the School District’s Acceptable Use Policy, other School District relevant policies, regulations, rules, and procedures, website and ISP terms, and local state and federal laws and procedures in cloud computing services.

8. Users must not store .exe files and/or install software in the School District’s cloud services.

9. As cloud solutions and security requirements continue to evolve, and laws change, students and employees must keep up to date and comply with them. Students and employees must be annually trained on cloud computing services, especially if there are upgrades or changes.

10. A backup system must be maintained to help protect against the loss of data and information that is in the cloud centralized servers. This may take the form of annual backup tapes, redundant hard drives, and/or duplicate server(s).

11. Access logs must be kept by IT personnel in order to identify unauthorized access or privacy or security breaches, and other issues. In addition, IT must monitor and apply daily hardware/software patch releases, obtain certifications from cloud vendors that security measures have been taken, encrypt transmitted data and information, and appropriately manage access to the cloud services by Users.

12. Retention and destruction of records must be kept in accordance with the School District’s Records Retention and Destruction Policy and Schedule.

13. Disciplinary consequences shall be in accordance with the School District’s policies, regulations, rules, and procedures, including but not limited to Student Discipline, Acceptable Use, Bullying/Cyberbullying, Harassment, Social Media, and other policies.

14. Violations of this Regulation must be reported to the Director of Technology, or designee.

**Guidelines**

1. 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.

1.1. 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.
1.2. 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.

1.3. 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.

1.4. Google Apps for Education (GAFE) is a cloud service. Employees and Guests must not use GAFE for School District Student Confidential, Sensitive, and Personally Identifiable Data and Information until or unless privacy and security protections are certified and approved.

1.5. 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.

References:
- *Breach of Personal Information Notification Act* (PA) – 73 P.S. § 2301 et seq.
- *HITECH Act* – 45 C.F.R. Part 160 and 164
- Identity Theft Laws (PA) – 18 Pa.C.S. § 4120; 42 Pa.C.S. § 9720.1
- *Confidentiality of Social Security Number* Law – 74 P.S. § 201
- CASD Board, Administrative Regulations, Rules, and Procedures, the *CASD Student Records Plan for the Collection, Maintenance, and Dissemination of Student Records*, the *CASD HIPAA Plan*, and the *CASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws*. 