SECTION: OPERATIONS

TITLE: CLOUD COMPUTING

ADOPTED: DECEMBER 15, 2014
2018

EAST STROUDSBURG AREA SCHOOL DISTRICT

816.1. CLOUD COMPUTING

1. Purpose

24 P.S. § 5-510

~~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 East Stroudsburg 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.~~

Users must prevent the East Stroudsburg Area School District ("School District") confidential, personally identifiable, sensitive, and proprietary data and information of students, employees, and the School District from being disclosed to unauthorized individuals and located in unprotected and unknown places.

The purpose of this policy is to address cloud issues relevant to Users and the School District. Data and information of the School District stored in clouds must be maintained to the levels of confidentiality, protection, security, and integrity that the School District, the law, and technology standards require.

The School District supports the use of cloud services that provide platforms, infrastructure, and services that maximize the business and educational communication, collaboration, data analysis, processing, sharing, management, and storage, but only with vendors/cloud providers who can provide the School District explicit protection restrictions on the storage of the School District's data and information as defined by the School District and the law.

Cloud computing services must be used solely for work purposes, and only cloud services approved by the Director of Technology may be used by Users. Furthermore, it is critical that Users do not open cloud services accounts or enter into cloud services contracts for cloud services without the approval of the Director of Technology. The protection, integrity and confidentiality of the data and information of the School District is vital.

2. Definition ESASD Policies	**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,/cloud providers and other who are using the School District's CIS systems[3] and cloud computing services.
3. Delegation of Responsibility	The superintendent must work in conjunction with the principals and Information Technology Department (IT) to create and implement an effective cloud computing system for School District 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 Policy. Users must be notified about, trained, and consent to the appropriate use of cloud computing services. Users who use the School District's CIS systems, clouds, ~~and/or~~ contracted cloud services, and information and data must comply with the School District's security requirements, including the School District's Acceptable Use Policy, Privacy and Security of Student Electronic and Digital Information Policy, Data Breach Notification Policy, other relevant School District policies, regulations, rules and procedures~~,~~; lawful website, cloud services, and ~~ISP~~Internet Service Providers' ("ISP") terms and conditions, and local, state and federal laws and procedures.

[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 offer and deliver more than one type of service. Generally, ~~T~~*the five "deployment models" include* (i) the private cloud, (ii) the community cloud, (iii) the public cloud, (iv) the 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."

4. Guidelines	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 a User must not place or keep School District information and data in a cloud service, or in virtual or online storage, beyond the control, access, protection, security, 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, and the User agrees to protect and ~~is~~be responsible for the privacy and security of School District information and data. 2. Anonymity of Users' activities sent to the cloud service provider must be a central aspect of protecting Users' privacy~~,~~. ~~m~~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 IT/Data Coordinator, or designee. 4. Access to data and information must be tiered within the cloud to those who have authorization and need to know the data and information. For example: School District high school principals~~administrators~~ may have access to the students' and teachers' data and information in their school, whereas teachers may have access to only their own students, and coaches may only have access to their players' data and information, 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 their child's~~student~~ records may be allowed by the use of guest passwords with specifically tailored access. 6. All content that Users post in School District authorized 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.
20 U.S.C. § 1232g	

7. Users must not post, possess, store, process, or transfer unlawful, threatening, libelous, defamatory, pornographic, child pornographic, obscene, harassing, bullying/cyberbullying, or other content that violates the School District's Acceptable Use Policy, other School District relevant policies, regulations, rules, and procedures, website, cloud services, and ISP terms, and local state and federal laws and procedures.

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

9. The cloud service provider's contract must at least indicate that the cloud service provider will (i) notify the School District about any privacy and/or security problems, and vulnerabilities (such as, but not limited to, hacking and other data integrity issues) of the cloud services; and (ii) will comply with all relevant federal, state, and local laws and regulations.

10. The School District must be aware of the potential for third-party vendors to profit from School District, employee, and student data and information. For example, some cloud providers might mine data for various purposes. Laws and regulations relevant to the data and information of the School District, employees, and students must be implemented.

11~~9~~. As privacy ~~cloud solutions~~ and security requirements of cloud solutions continue to evolve, and laws change ~~students and employees~~Users must keep up-to-~~-~~date and comply with them. Users~~Students and employees~~ must be annually educated about~~trained on~~ cloud computing services, especially if there are upgrades or changes.

12~~0~~. A backup system must be maintained to help protect against the loss of data and information that is in the cloud servers. This may take the form of annual backup tapes, redundant hard drives, ~~and/or~~ duplicate server(s), and/or other service authorized by the School District.

13~~1~~. Access logs must be kept by IT personnel in order to identify unauthorized access or privacy or security breaches, ~~and~~as well as other issues. In addition, IT must monitor and apply daily hardware/software patch releases, obtain certifications from cloud ~~vendors~~providers confirming that security measures have been taken, encrypt transmitted data and information, and appropriately manage access to the cloud services by Users.

14~~2~~. Retention and destruction of records must be kept in accordance with the School District's Records Retention and Records Destruction Policy and Schedule.

15~~3~~. 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.

16. Users who violate this policy are also subject to other School District applicable policies, regulations, rules and procedures. Any User who violates this policy is subject to disciplinary action, up to and including termination of their relationship with the School District. Furthermore, the User may be subject to a legal action, and may be held financially responsible for the costs incurred as a result of a data breach, loss, or illegal disclosure. Anyone viewing, updating, or releasing School District data or information for any reason other than officially authorized School District business may be held personally liable and subject to criminal and civil penalties.

14. Violations of this Policy must be reported to the ~~Director of Technology~~Superintendent, and/or designee.

References:

~~*-Family Educational Rights and Privacy Act – 20 U.S.C. § 1232 (g), 34 C.F.R. § 99.1 et seq.*~~

-The NIST Definition of Cloud Computing, Special Publication 800-145, National Institute of Standards and Technology, U.S. Department of Commerce, Sept. 2011.

-The Center for Internet Security's Critical Security Controls

-American Recovery and Reinvestment Act of 2009 (ARRA), §13402(h)(2).

~~*-Breach of Personal Information Notification Act (PA) – 73 P.S. § 2301 et seq.*~~

-Fair Credit Reporting Act – 15 U.S.C. § 1681a

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

-HITECH Act – 45 C.F.R. Part 160 and 164

-Breach of Personal Information Notification Act (PA) – 73 P.S. § 2301 et seq.

-Confidentiality of Social Security Law – 74 P.S. § 201

-Identity Theft Laws (PA) – 18 Pa. C.S. § 4120; 42 Pa. C.S. § 9720.1

- Pennsylvania Student Records law – 22 Pa. Code § 12.31 - §12.32

~~*-Confidentiality of Social Security Law – 74 P.S. § 201*~~

- ESASD Board, Administrative Regulations, Rules, and Procedures

-The ESASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws

-The ESASD HIPPA Plan

-ESASD Records Retention and Records Destruction Policy, and accompanying Schedule

-The ESASD Student Records Plan for the Collection, Maintenance, and Dissemination of Student Records

~~*-The ESASD HIPPA Plan*~~

~~*-The ESASD Checklist for Responding to Reported and Suspected Data Security Breaches: Data Breach Notification Laws*~~