Business and Non-Instructional Operations

STUDENT DATA PROTECTION AND PRIVACY / CLOUD-BASED ISSUES 3520.13(a)

The District may, pursuant to this policy, enter into a contract with a third party for either or both of the following purposes:

1. To provide services, including Cloud-based services, for the digital storage, management, and retrieval of student records.

2. To provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use student records in accordance with the contractual provisions listed below.

The District, when entering into a contract with a contractor for purposes listed above, shall ensure the contract includes, but is not limited to the following:

1. A statement that student records, student information and student generated content continues to be the property of and under the control of the District. (They are not the property of, or under the control of a software or electronic service contractor.)

2. A description of the means by which the District, students, their parents or legal guardians, may retain possession and control of student-generated content, and if applicable, means by which a student, parent or legal guardian of a student may transfer student-generated content to an electronic mail account.

3. A statement that the contractor will not use student information, student records, or student-generated content for any purposes except those the contract authorizes.

4. A description of the procedures by which a student, parent or legal guardian, of a student may review personally identifiable information (PII) contained in the student's record, student information or student-generated content and correct erroneous information, if any in such student material.

5. A statement that the contractor shall take actions designed to ensure the security and confidentiality of student records, student information, and student-generated content.

6. A description of the procedures that a contractor will follow for notifying a student, the parent or legal guardian of a student, and the District, as soon as practical, but not later than forty-eight (48) hours after the contractor becomes aware of or suspects that any student record, student information, or student-generated content under the contractor's control has been subject to unauthorized access or suspected unauthorized access.

Business and Non-Instructional Operations

STUDENT DATA PROTECTION AND PRIVACY / CLOUD-BASED ISSUES (continued) **3520.13(b)**

7. A statement that a student's records, student information, or student-generated content shall not be retained or available to the contractor upon completion of the contracted services unless a student, parent or legal guardian of a student chooses to establish or maintain an electronic account with the contractor for the purpose of storing student-generated content. (e.g. – essays, research papers, portfolios, creative writing, music, audio files, or photographs, but not standardized assessment responses.)
8. A statement that the contractor and the District shall ensure compliance with the federal Family Educational Rights and Privacy Act (FERPA), 20 USC 1232g.
9. A statement that Connecticut laws shall govern the rights and duties of all parties to the contract, (contractor and the District).
10. A statement that if any provision of the contract or the application of the contract is held invalid by a court of competent jurisdiction, the invalidity does not affect other provisions of the contract which can be given effect without the invalid provision or application.
11. A prohibition against the contractor using personally identifiable information contained in student records to engage in advertising or for any other purposes other than those authorized pursuant to the contract.

Any provision of a contract entered into between a contractor and the District that conflicts with the provisions listed above shall be void. Moreover, a contract is void if it lacks any of the above provisions. The District will give the contractor reasonable notice to amend the contract to include the missing provisions.

Any contract entered into that does not include the provisions listed above shall be void, provided the District has given reasonable notice to the contractor and the contractor has failed within a reasonable time to amend the contract to include the required provisions.

Not later than five business days after executing a contract pursuant to this policy, the District shall provide electronic notice to any student and the parent or legal guardian of a student affected by the contract. The notice shall (1) state that the contract has been executed and the date that such contract was executed, (2) provide a brief description of the contract and the purpose of the contract, and (3) state what student information, student records or student-generated content may be collected as a result of the contract. The District shall post such notice and the contract on the District's Internet website.

Business and Non-Instructional Operations

STUDENT DATA PROTECTION AND PRIVACY / CLOUD-BASED ISSUES (continued) **3520.13(c)**

The District expects that an operator shall implement and maintain reasonable security procedures and practices to protect student information from unauthorized access, destruction, use, modification and disclosure; that, based on the data's sensitivity and risk from unauthorized access, do the following:

1. Use technology and methodologies consistent with guidance issued about protected health information under the federal Health Information Technology for Economic and Clinical Health Act of 2009. (HITECH Act),
2. Maintain technical safeguards for student records in a manner consistent with federal HITECH Act regulations on technical safeguards for electronic protected Health Information, and
3. Otherwise meet or exceed industry standards.

Notice of Breach of Security/Data Breacher

Upon notice of a breach of security by a contractor, the District shall, within forty-eight (48) hours notify the students and the parents/legal guardians of the students whose student information, student records, or student-generated content was involved in such breach. The District shall also, as required, post notice of the breach on its website.

Upon the discovery of a breach of security that results in the unauthorized release of student information, excluding directory information, the contract shall contain the provision that the contractor must notify the District of such breach without unreasonable delay, and in no case later than thirty (30) days from the discovery of the breach.

Upon the discovery of a breach of security that results in the unauthorized release of directory information, student records, or student-generated content, the contract shall contain the provision that the contractor must notify the District without unreasonable delay and in no case later than sixty (60) days from the discovery of the breach.

Definitions

1. **"Contractor"** means an operator or consultant that is in possession of or has access to student information, student records or student-generated content as a result of a contract with a local or regional District of Education.
2. **"Operator"** means the operator of an Internet website, online service, online application, (app) or mobile application with actual knowledge that such Internet website, service, or mobile application is used primarily for school purposes and was designed and marketed for school purposes and who collects, maintains or uses student information.

Business and Non-Instructional Operations

STUDENT DATA PROTECTION AND PRIVACY / CLOUD-BASED ISSUES **3520.13(d)**

Definitions (continued)

3. **"Consultant"** means a professional who provides non-instructional services, including administrative, planning, analytical, statistical, or research services to a District of education under a contract.
4. **"Student"** means a Connecticut resident enrolled in a preschool program participating in the state-wide public school information system, pursuant to section 10-10a of the general statutes, or enrolled in grades K to 12, inclusive, in a public school, or receiving special education and related services under an individualized education program, or otherwise the responsibility of the District.
5. **"Deidentified information"** means any information that has been altered to prevent the identification of an individual student.
6. **"Eligible student"** means a student who has reached 18 years of age.
7. **"Student-generated content"** means materials created by a student, including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, or photographs. "Student-generated content" does not include student responses to a standardized assessment.
8. **"Student records"** means any information directly related to a student that is maintained by the school district, the State District of Education or the Department of Education or any information acquired from a student through the use of educational software assigned to the student by a teacher or other district employee.

   "Student records" does not mean any of the following:

   a. Deidentified information, allowed under the contract to be used by the contractor to improve educational products for adaptive learning purposes and for customizing student learning.
   b. Deidentified information, used to demonstrate the effectiveness of the contractor's products in the marketing of such products.
   c. Deidentified information, used for the development and improvement of the contractor's products and services.
9. **"Online service"** includes Cloud computing services, which must comply with this policy if they otherwise meet the definition of an operator.
10. **"Student information"** is personally identifiable information regarding a student that in any media or format that is not publicly available that meets any of the following:

    a. Is created or provided by a student, or the student's parent or legal guardian, by using an operators' website, online service, or mobile application (app) for school purposes.

Business and Non-Instructional Operations

STUDENT DATA PROTECTION AND PRIVACY / CLOUD-BASED ISSUES **3520.13(e)**

Definitions (continued)

b. Is created or provided by an employee or agent of the District of education, to an operator for school purposes.

c. Is gathered by an operator through the operation of the operator's Internet website, online service, or mobile application (app) and identifies a student including but not limited to information in the student's educational record or email account, first and last name, home address, telephone number, date of birth, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or behavioral assessments.

11. **"School purposes"** means purposes that customarily take place at the direction of a teacher, or the District, or aid in the administration of school activities, including, but not limited to, instruction in the classroom, administrative activities, and collaboration among students, school personnel, or parents/legal guardians.

12. **"Targeted advertising"** means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student-generated content or inferred from the usage of the operator's Internet website, online service or mobile application by such student. It does not include any advertising to a student on a website that the student accesses at the time or in response to a student's response or request for information or feedback.

The District, through this policy, places restrictions on an "operator" as defined in this policy. An operator shall not knowingly engage in any of the following activities with respect to their internet website, online service or mobile application:

1. Engage in targeted advertising on the operator's site, service, or application, or on any other Internet website, online service or mobile application;
2. Use student information to create a profile of a student for purposes other than the furtherance of school purposes;

Business and Non-Instructional Operations

STUDENT DATA PROTECTION AND PRIVACY / CLOUD-BASED ISSUES (continued) **3520.13(f)**

3. Sell student information, unless the sale is part of the purchase, merger, or acquisition of an operator by a successor operator and the operator and the successor operator continue to be subject to the provisions of this policy regarding student information; or
4. Disclose student information, unless the disclosure is made (a) in furtherance of school purposes of the Internet website, online service or mobile application, provided the recipient of the student information uses such student information to improve the operability and functionality of the Internet website, online service or mobile application and complies with this policy; (b) to ensure compliance with federal or state law; (c) in response to a judicial order; (d) to protect the safety of users or others, or the security of the Internet website, online service or mobile application; or (e) to an entity hired by the operator to provide services for the operator's Internet website, online service or mobile application, provided the operator contractually (i) prohibits the entity from using student information for any purpose other than providing the contracted service to, or on behalf of, the operator, (ii) prohibits the entity from disclosing student information provided by the operator to subsequent third parties, and (iii) requires the entity to comply with this policy.

The District recognizes that an operator may:

1. Use student information (a) to maintain, support, evaluate or diagnose the operator's Internet website, online service or mobile application (app), or (b) for adaptive learning purposes or customized student learning.
2. Use de-identified student information (a) to develop or improve the operator's Internet website, online service or mobile application (app), or other Internet websites, online services or mobile applications owned by the operator, or (b) to demonstrate or market the effectiveness of the operator's Internet website, online service or mobile application.
3. Share aggregated de-identified student information for the improvement and development of Internet websites, online services or mobile applications designed for school purposes.

Nothing in this policy shall be construed to:

1. Limit the ability of a law enforcement agency to obtain student information from an operator as authorized by law or pursuant to a court order;
2. Limit the ability of a student or the parent or legal guardian of a student to download, transfer or otherwise save or maintain student information;
3. Impose a duty upon a provider of an interactive computer service, as defined in 47 USC 230, as amended from time to time, to ensure compliance with this section by third-party information content providers, as defined in 47 USC 230, as amended from time to time;

Business and Non-Instructional Operations

STUDENT DATA PROTECTION AND PRIVACY / CLOUD-BASED ISSUES (continued) **3520.13(g)**

4. Impose a duty upon a seller or provider of online services or mobile applications to ensure compliance with this policy with regard to such online services or mobile applications;
5. Limit an Internet service provider from providing a student, parent or legal guardian of a student or local or regional District of Education with the ability to connect to the Internet;
6. Prohibit an operator from advertising other Internet websites, online services or mobile applications that are used for school purposes to parents or legal guardians of students, provided such advertising does not result from the operator's use of student information; or
7. Apply to Internet websites, online services or mobile applications that are designed and marketed for use by individuals generally, even if the account credentials created for an operator's Internet website, online service or mobile application may be used to access Internet websites, online services or mobile applications that are designed and marketed for school purposes.

The District, upon determination that a request for directory information is related to school purposes, may disclose directory information to any person requesting such directory information. If the District determines that a request for directory information is not related to school purposes, the District shall not disclose such directory information.

(cf. 3520.1 – Information Security Breach and Notification)
(cf. 3520.11 – Electronic Information Security)
(cf. 3520.12 – Data-Based Information Management System Confidentiality Policy)
(cf. 5125 – Student Records)
(cf. 5145.15 – Directory Information)
(cf. 6162.51 – Surveys of Students/Student Privacy)

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.
7-109 Destruction of documents.
10-15b Access of parent or guardians to student's records.
10-209 Records not to be public.
11-8a Retention, destruction and transfer of documents
11-8b Transfer or disposal of public records. State Library District to adopt regulations.
46b-56(e) Access to Records of Minors.

Business and Non-Instructional Operations

STUDENT DATA PROTECTION AND PRIVACY / CLOUD-BASED ISSUES (continued) **3520.13(h)**

Legal Reference: (continued)

Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).
P.A. 16-189 An Act Concerning Student Privacy
Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of P.L. 93-568, codified at 20 U.S.C.1232g).
Dept. of Educ, 34 C.F.R. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Educ. Provisions Act (20 U.S.C. 1232g) parent and student privacy and other rights with respect to educational records, as amended 11/21/96.
Protection of Pupil Rights Amendment (PPRA) 20 U.S.C. § 1232g (2014)
Children's Online Privacy Protection Act (COPPA) 15 U.S.C. §§6501 *et seq.* (2014)

Adopted 1/10/2017