BOARD OF EDUCATION
FAIRFIELD PUBLIC SCHOOLS
FAIRFIELD, CT

Policy Committee Meeting

Monday, October 10, 2016
4:30 p.m.
501 Kings Highway East
Superintendent's Conference Room

Agenda

I. Call to Order

II. Approval of September 26, 2016 Meeting Minutes

III. Policy

3520.12 – Data-Based Information Management System Confidentiality
3520.13 Student Data Protection and Privacy / Cloud-Based Issues

IV. Open Discussion/Public Comment

V. Adjournment

VI. Future Items

Future Mtg. Dates and Times: *All meetings will be on Mondays, starting at 4:30 unless otherwise noted:* November 7, December 5, 2016.

All meetings will be held at 501 Kings Highway East, Superintendent's Conference Room unless otherwise noted.

DRAFT

BOARD OF EDUCATION
FAIRFIELD PUBLIC SCHOOLS
FAIRFIELD, CT

Policy Committee Meeting

Monday, September 26, 2016
4:30 p.m.
501 Kings Highway East
Superintendent's Conference Room

Minutes

I. Call to Order The meeting was called to order at 4:40 PM. In attendance: J. Kennelly (Chair), D. Karnal, A. Calabrese, J. Coyne (for the Administration)

II. Approval of September 12, 2016 Meeting Minutes Approved 3-0

III. Policy

- Policy #5111 Students – Admission/Placement
(Replacement for existing Policy#5111) *Committee reviewed and discussed this policy from CABE for the second time. Changes were made based on some information from CABE. Committee approved the policy with edits to move to full Board for first reading at the next BOE meeting. 3-0*

- Policy #5112 Students – Attendance/Excuses/Dismissal
(Recodified to CABE 5113, with required addition of sections required by PA 15-225. Existing policies 5116, 5121, and 5114 have been made a part of this policy.) *Committee reviewed and discussed this policy for the second time. Minor edits were made and the policy was approved to send to the full Board for first reading at the next BOE meeting. 3-0. Athe committee will also be proposing the deletion of # 5116, 5121, and 5114 when the # 5113 comes up for a vote by the BOE.*

IV. Open Discussion/Public Comment *No public comment. Mrs. Kennelly stated that the committee was eager to see more policies from the CABE audit for review.*

V. Adjournment *The meeting adjourned at 5:21 PM 2-0 (Mr. Calabrese left a few minutes before adjournment).*

VI. Future Items *More policies identified by the CABE audit.*

Future Mtg. Dates and Times: *All meetings will be on Mondays, starting at 4:30 unless otherwise noted:* October 10, November 7, December 5, 2016.

All meetings will be held at 501 Kings Highway East, Superintendent's Conference Room unless otherwise noted.

An optional sample policy to consider.

Business and Non-Instructional Operations

Data-Based Information Management System

Confidentiality Policy

It is the policy of the _____District to respect the privacy, dignity, and confidentiality of all students attending the _____School District. This policy covers student records, medical information, and other personally identifiable sources of information. It is the policy of the District that such personally identifiable information should only be viewed or received by School District employees who have a legitimate educational interest in viewing or receiving the information, as well as those officials involved in a supervisory capacity over the school in which the students are enrolled. This policy shall not apply to the District's library records, including Internet logs, the disclosure of which shall be regulated by state and federal law.

Student Records and Personally Identifiable Information

It is the policy of the District that the building Principal of each school, or his/her designee, shall be the custodian of all student records for that school. The District will only release records in accordance with the provisions of the Family Educational Rights and Privacy Act of 1974 ("FERPA"), as well as other relevant federal and state mandates as they relate to student records, personally identifiable information, and confidentiality. Accordingly, the District will only release personally identifiable information, other than directory information defined herein, to the following individuals or situations:

1. School officials, who have been determined by such agency or institution to have legitimate educational interests in the records.
2. Officials of another public school, including a public charter school, in which the student seeks or intends to enroll. Disclosure of personally identifiable information will be made only upon condition that the student's parents be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record.
3. Authorized representatives of the Comptroller General of the United States; the Attorney General of the United States; the Secretary of Education; or state and local educational authorities, under the following conditions; the school shall provide such authorized representatives access to student or other records that may be necessary in connection with the audit, evaluation, or enforcement of State and federally supported education programs, but shall not permit such representatives to collect personally identifiable information unless specifically authorized to do so by state and federal law or if the parent or eligible student has given written consent for the disclosure.
4. In connection with a student's application for, or receipt of, financial aid, if such information is necessary to determine eligibility for, the amount of, or the conditions for financial aid, or to enforce the terms and conditions of financial aid.

Business and Non-Instructional Operations

Data-Based Information Management System

Confidentiality Policy

Student Records and Personally Identifiable Information (continued)

5. State and local officials or authorities to whom such information is specifically required to be reported or disclosed pursuant to state statute adopted prior to November 19,1974, if the disclosure concerns the juvenile justice system and its ability effectively to serve the student whose records are released. If reporting or disclosure is permitted pursuant to a state statute concerning the juvenile justice system adopted after November 19, 1974, such disclosure may be made without consent only if the officials and authorities to whom the records are disclosed certify in writing to the school district that the information will not be disclosed to any other party without the prior, written consent of the parent of the student, except as provided under State law.

6. Organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, or improving instruction, so long as the study does not permit personal identification of parents or students by individuals other than representatives of the organization and the information is destroyed after it is no longer needed for the purposes for which the study was conducted.

7. Accrediting organizations in order to carry out their accrediting functions.

8. Parents of an eligible student who claim that student as a dependent student as defined in Section 152 of the Internal Revenue Code of 1986.

9. Disclosure is required to comply with a judicial order or lawfully issued subpoena, provided that the educational agency makes a reasonable effort to notify the parent or the eligible student in advance of compliance, unless such disclosure is in compliance with (a) a federal grand jury subpoena and the court has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed; or (b) any other subpoena issued for a law enforcement purpose and the court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed.

10. Disclosure is required in connection with a health and safety emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals.

11. Between two or more public schools in which the student is enrolled or receiving services.

Business and Non-Instructional Operations

Data-Based Information Management System

Confidentiality Policy

Student Records and Personally Identifiable Information (continued)

12. If the school district initiates legal action against a parent or student, the school district may disclose to the court, without a court order or subpoena, the education records of the student that are relevant for the school district to proceed with the legal action as plaintiff.

13. If a parent or eligible student initiates legal action against the school district, the school district may disclose to the court, without a court order or subpoena, the student's educational records that are relevant for the school district to defend itself.

14. To the Attorney General of the United States or his/her designee in response to an ex parte order in connection with the investigation or prosecution of terrorism crimes specified in sections 2332b(g)(5)(B) and 2331 of Title 18, U.S. Code.

Employees of the District who have access to personally identifiable information shall keep such information confidential and shall not share such information with others who do not have a legitimate educational interest in such information. When receiving an inquiry from individuals who are not specifically known to be qualified to receive the information, the employee shall consult the "Student Records" policy, #5125, prior to the disclosure of any personally identifiable information, to determine if the individual seeking such information is listed as a person entitled to receive such information. The employee shall not disclose any information until appropriate written authorization has been received. The building Principal for each school, or his/her designee, shall make the final determination about whether an employee of the District has a legitimate educational interest in personally identifiable information.

Employees receiving personally identifiable information shall safeguard the information from dissemination to unauthorized parties. Steps should be taken to insure that personally identifiable information does not accidentally find its way into the public domain. Personally identifiable information that is no longer needed should be destroyed as soon possible, provided that appropriate and adequate back-ups of such information exist in accordance with the District's storage and student record retention policies.

Business and Non-Instructional Operations

Data-Based Information Management System

Confidentiality Policy (continued)

Medical Records and/or Information

Medical records and/or information shall only be shared with school officials and employees who have a legitimate "need to know" such information. Such medical information shall be safeguarded while in the possession of school officials/employees. Once the circumstances giving rise to the "need to know" no longer exist, the school official or employee shall immediately destroy the information in a manner that will insure the continued privacy and confidentiality of such information. The only exception to this rule shall be the student's master health record and/or the student's 504/special education file, which may contain information about prior medical conditions that may no longer be active but may be relevant to future treatment/programming decisions.

Medical information shall only be shared with non-school officials/employees who are authorized to review such information. Medical information shall not be disclosed to individuals who have not received prior written authorization, except as otherwise permitted by law. Nothing herein shall be construed to prevent District officials from sharing information with emergency medical personnel as necessary to insure the health, safety, and well-being of any student or employee of the School District. Further, medical information may be shared with non-School District employees who have responsibility for the protection of students in their custody.

Directory Information

The District will, unless otherwise directed by an eligible student and/or parent(s), prepare directory information regarding each student. Directory information shall include the following:

a. the student's name
b. the student's class designation
c. the student's extra-curricular activities
d. the name of the school the student is currently attending
e. achievement awards or honors
f. height, weight, performance of members of athletic teams
g. street address or postal box number[1]

[1] Subject to Superintendent approval, organizations involved with school-sponsored activities (i.e. Washington trip) may be provided with student addresses for the purposes of notifying students and/or parents of pertinent information.

Business and Non-Instructional Operations

Data-Based Information Management System

Confidentiality Policy

Directory Information (continued)

Directory information may be published in student yearbooks, School District web sites, athletic publications, radio programs, television broadcasts, performing group graduation programs, and in the publication of achievement awards and honors for individual students. This information may also be disseminated to local newspapers in accordance with school sponsored sporting activities and/or programs. Unless otherwise directed by the student or parents involved, such directory information shall be available as specified herein.

Observations

During the course of carrying out activities as an employee or volunteer of the District, individuals may make certain observations that may disclose personally identifiable information about a student. These observations may indicate the nature of disabilities and/or accommodations that are made in response to such disabilities. These observations, by their very nature, may result in the employee or the volunteer receiving information in which they neither have any legitimate educational interest nor a "need to know." To the degree such observations disclose personally identifiable information; the employee or volunteer in question making such observations must respect the privacy, dignity, and confidentiality of the student involved and not disclose such information in violation of this policy.

Violations

The dissemination of personally identifiable information by employees or volunteers to individuals who have neither a legitimate educational interest nor a "need to know" is strictly prohibited. Further, employees or volunteers are not to disclose such personally identifiable information to individuals who are not affiliated with the District without specific written authorizations for the release of such information. If the employee or volunteer has any question as to whether the individual is entitled to receive such information, then the building Principal or designee shall be consulted prior to disclosure.

Employees or volunteers who release personally identifiable information in violation of this policy shall be subject to discipline and/or exclusion from continuing participation in volunteer activities. Such discipline may include, but not be limited to, termination.

Business and Non-Instructional Operations

Data-Based Information Management System

Confidentiality Policy (continued)

Electronic Records/Information

Employees who have access to electronic personally identifiable information shall safeguard the dissemination of such material in accordance with this policy. In particular, information shall not be forwarded to individuals who do not have a legitimate educational interest in the information or a "need to know." Further, personally identifiable information shall not be stored in a manner in which unauthorized students, employees, or third parties may gain access.

Employees who maintain the District's computer system, software or electronic databases shall take sufficient steps to secure the databases from unauthorized access to personally identifiable information. Further, such employees shall not access personally identifiable information unless they possess the requisite need to know. Personally identifiable information that is encountered by such employees through ordinary upkeep and maintenance of the District's computer system, software or databases should not be read for content unless absolutely necessary. To the degree such information is inadvertently obtained, employee shall keep such information confidential and shall not disclosure the information to unauthorized individuals.

When using email as a means of communicating personally identifiable information, employees shall take all steps to insure that the email addresses are accurate and that the information is not inadvertently delivered to unauthorized individuals. Further, and to the degree that information is going to be shared amongst a large group, information shall be tailored so that personally identifiable information is not shared with individuals without a legitimate educational interest or a "need to know." Electronic records containing personally identifiable information should be destroyed and/or deleted as soon as the information is no longer needed, provided that appropriate and adequate backups of such information exist in accordance with the District's storage and student record retention policies.

Definitions

A. **Personal Information.** This is information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a social security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number, or a health insurance identification number.

or: *Personally identifiable information includes, but is not limited to, the name and address of the student, student's parent, or other family member, the student's personal identifier, such as social security number or student identification number, or a list of characteristics or other information that would make the student's identity easily traceable.*

Business and Non-Instructional Operations

Data-Based Information Management System

Confidentiality Policy

Definitions (continued)

B. **Legitimate Educational Interest.** A school official with a "legitimate educational interest" shall be deemed to include incumbent school board members, Superintendent of Schools, principal, assistant principal, guidance counselor, teacher(s) and/or aides of the student, nurse, school medical advisor/physician, and any members of a diagnostic and placement team who have responsibility for developing an appropriate educational program for the student.

C. **Need To Know.** School officials with a "need to know" shall be deemed to include incumbent school board members, Superintendent of Schools, principal, assistant principal, guidance counselor, teacher(s) and/or aides of the student, nurse, school physician, and any members of a diagnostic and placement team who have responsibility for developing an appropriate educational program for the student, Further, employees with a "need to know" shall be deemed to include such other employees of the District who's involvement or responsibility for the safety and well-being the student in question, or other students, requires the disclosure of personally identifiable information. Such employees may include, but are not limited to, bus drivers, transportation aides, athletic personnel, school resource officer, and cafeteria monitors etc.

D. **Eligible Student.** The term "eligible student" shall be deemed to pertain to a student that has reached the age of majority or a student who has been legally emancipated. Notwithstanding, personally identifiable information, including academic performance, attendance, disciplinary events, medical matters shall continue to be shared with the parent(s) of an "eligible student" until such time as the District is directed by the "eligible student", in writing, not to disclose such information to the parents.

(cf. 3520 – Data-Based Information Management System)
(cf. 3520.1 – Information Security Breach and Notification)
(cf. 3520.11 – Electronic Information Security)
(cf. 3543.31 – Electronic Communications Use and Retention)
(cf. 5125 – Student Records; Confidentiality)
(cf. 5125.11 – Health/Medical Records (HIPAA))

Business and Non-Instructional Operations

Data-Based Information Management System

Confidentiality Policy

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.

10-154a Professional communications between teacher or nurse & student.

10-209 Records not to be public.

10-221b Boards of education to establish written uniform policy re: treatment of recruiters.

11-8a Retention, destruction and transfer of documents

11-8b Transfer or disposal of public records. State Library Board to adopt regulations.

46b-56 (e) Access to Records of Minors.

Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).

P.A. 08-160: An Act Concerning the Confidentiality of Social Security Numbers

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.

USA Patriot Act of 2001, PL 107-56, 115 Stat. 272, Sec 507, 18 U.S.C. §2332b(g)(5)(B) and 2331

PL 107-110 “No Child Left Behind Act of 2001” Sections 5208 and 9528

Policy adopted:

cps 1/09

P.A. 16-189 An Act Concerning Student Data Privacy

(Background Information for Policy Review Committee)

Summary: This Act restricts how student information, student records, or student-generated content may be used by (1) contractors that provide student data services to boards of education and (2) certain operators of websites, online services, or mobile applications ("apps").

For contractors, the Act establishes requirements for contract content; contract execution notice to parents and guardians; and protection, deletion, and use of student information.

The Act requires operators of websites, online services, or apps to maintain reasonable security practices to protect student information and delete student information upon student, parent, guardian, or board of education request. It prohibits, with some exceptions, operators from engaging in targeted advertising, creating student profiles for purposes unrelated to school, or selling or disclosing student information. However, the Act allows operators to use some student information and de-identified student information for purposes related to student learning or product operational improvements.

The Act also prescribes how contractors and operators must respond to security breaches involving student information, directory information, student records, or student-generated content in their possession.

Additionally, the Act establishes a task force to study student data privacy issues.

This Act becomes effective October 1, 2016, except the provisions about (1) contracts apply to contracts entered into, amended, or renewed on or after October 1, 2016 and (2) the task force take effect upon passage.

§ 1 - DEFINITIONS

Parties Defined

The Act defines a **"contractor"** as an operator or consultant that possesses or has access to student information, student records, or student-generated content as a result of a written contract with a local or regional board of education. An **"operator"** is anyone who (1) operates a website, online service, or app with actual knowledge that such website, service, or app is used for and was designed and marketed for school purposes, to the extent that it is engaged in its operation, and (2) collects, maintains, or uses student information. A **"consultant"** is a professional who provides non-instructional services, including administrative, planning, analytical, statistical, or research services to a board of education under a contract.

The Act defines a **"student"** as a Connecticut resident who is (1) enrolled in a preschool program participating in the statewide public school information system, (2) enrolled in grades kindergarten through 12 in a public school, (3) receiving special education services under an individualized education program, or (4) otherwise the responsibility of a board of education.

Related Terms Defined

The Act defines "**school purposes"** as purposes that (1) customarily take place at the direction of a teacher or a board of education or (2) aid in the administration of school activities, including (a) classroom instruction, (b) administrative activities, and (c) collaboration among students, school personnel, or students' parents or legal guardians.

"**Student information**" is personally identifiable information or student material in any media or format that is not publicly available and is any of the following:

1. created or provided by a student or a student's parent or legal guardian by using an operator's website, online service, or app for school purposes;
2. created or provided by an employee or agent of a board of education to an operator for school purposes; or
3. gathered by an operator through its website, online service, or app and identifies a student, including (a) information in the student's records or email account; (b) first or last name; (c) home address or telephone number; (d) date of birth; (e) email address; (f) discipline records; (g) test results; (h) grades; (i) evaluations; (j) criminal, medical, or health records; (k) Social Security number; (l) biometric information; (m) disabilities; (n) socioeconomic information; (o) food purchases; (p) political or religious affiliations; (q) text messages; (r) documents; (s) student identifiers; (t) search activity; (u) photographs or voice recordings; (v) survey responses; or (w) behavioral assessments.

The Act defines a "**student record"** as any information (1) directly related to a student that boards of education, the State Department of Education, or the State Board of Education maintains or (2) acquired through a student's use of educational software that a teacher or other public education employee assigned. It does not include de-identified student information that the contract permits the contractor to use for any of the following purposes:

1. improving educational products for adaptive learning purposes and for customizing student learning,
2. demonstrating the product's effectiveness for marketing purposes, and
3. developing and improving the contractor's products and services.

"De-identified student information" is any student information that has been altered to prevent identification of an individual student.

The Act defines **"targeted advertising**" as presenting an advertisement to a student where the selection of the advertisement is (1) based on student information, student records, or student-generated content or (2) inferred over time from the (a) student's use of the operator's website, online services, or app or (b) retention of the student's online activities or requests over time for the purpose of targeting subsequent advertisements. 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.

§ 2 - CONTRACTORS

The Act establishes requirements for contractors who provide student data services to boards of education, specifically about contract content, notice of contract execution, protection and deletion of student information, and restrictions on use of student information. It applies to contracts entered into, amended, or renewed on or after October 1, 2016.

Required Contract Contents

Beginning October 1, 2016, the Act requires boards of education to enter into a written contract with any contractor with whom it shares or provides access to student information, student records, or student-generated content. The contract must state the following:

1. student records, student information, and student-generated content are not the property of, or under the control of, a contractor;
2. the contractor will not use student information, student records, and student-generated content for any purposes except those the contract authorizes;
3. the contractor must take actions designed to ensure security and confidentiality of student information, student records, and student-generated content;
4. the contractor will not retain or have available student information, student records, or student-generated content after completing the contracted services unless a student, parent, or guardian chooses to establish or maintain an electronic account with the contractor to store student-generated content (e. g., essays, research papers, portfolios, creative writing, music, audio files, or photographs, but not standardized assessment responses);
5. the contractor and the board of education must ensure compliance with the federal Family Educational Rights and Privacy Act of 1974 (FERPA);
6. Connecticut law governs the rights and duties of all parties to the contract; and
7. a court finding of invalidity of any contract provision does not invalidate other contract provisions or applications not affected by the finding.

The contract must also describe the following:

1. how the board of education may request deletion of student information, student records, or student-generated content in the contractor's possession;
2. procedures for a student, parent, or guardian to (a) review personally identifiable information in student information, student records, and student-generated content and (b) correct erroneous information, if any, in the record; and
3. procedures that a contractor will follow to notify the board of education when there has been an unauthorized release, disclosure, or acquisition of student information, student records, or student-generated content.

Under the Act, a contractual provision is void if it conflicts with any of the above 10 provisions. Similarly, a contract is void if it lacks any of the above 10 provisions. However, the board of education must give the contractor reasonable notice to amend the contract to include the missing provisions.

Notice of Contract Execution

The Act requires boards of education to electronically notify affected students and their parents or guardians within five business days after entering into a contract with a contractor. The notice must (1) state that the contract has been executed and its date of execution; (2) provide a brief description of the contract and its purpose; and (3) state what student information, student records, or student-generated content may be collected under the contract. The Act also requires boards of education to post the notice and contract on their websites.

Requirement to Protect and Delete Student Information

Under the Act, a contractor must implement and maintain security procedures and practices designed to protect student information from unauthorized access, destruction, use, modification, or disclosure that, based on the data's sensitivity and risk from unauthorized access, do the following:

1. use technologies 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.

Restrictions on Contractors

The Act bans contractors from using (1) student information, student records, or student-generated content for any purposes other than those the contract authorizes or (2) personally identifiable information contained in student information, student records, or student-generated content to engage in targeted advertising. The Act specifies that all student-generated content is the property of the student or his or her parents or guardians.

§ 3 - OPERATORS

Under the Act, operators of Internet websites, online services, and apps must meet several security requirements and abide by various restrictions on the use of student information, records, and student-generated content. However, the Act permits operators to disclose and share such data under certain circumstances.

Operator Requirements

The Act requires operators to do the following:

1. implement and maintain security procedures and practices that meet or exceed industry standards and are designed to protect student information, student records, and student-generated content from unauthorized access, destruction, use, modification, or disclosure; and
2. delete any student information, student records, or student-generated content within a reasonable amount of time if requested by a student, parent, or guardian or a board of education that has the right to control such student information.

Operator Restrictions

The Act prohibits operators from knowingly doing the following:

1. collecting, storing, and using student information, student records, student-generated content, or persistent unique identifiers, except to further school purposes;
2. selling, renting, or trading student information, student records, or student-generated content unless the sale is part of the purchase, merger, or acquisition of an operator by a successor operator, and the successor operator continues to be subject to the act's provisions;
3. disclosing student information, student records, or student-generated content, with some exceptions (see below); or
4. engaging in targeted advertising on (a) the operator's website, online service, or app or (b) any other website, service, or app if the advertising is based on student information, student records, student-generated content, or persistent unique identifiers the operator acquired through the use of the operator's website, service, or mobile app for school purposes.

The Act defines "**persistent unique identifier"** as a unique piece of information that (1) can be used to recognize a user over time and across different websites, online services, or apps and (2) is acquired as a result of a student's use of an operator's website, online service, or app.

Permissible Disclosures

The Act permits operators to disclose student information, student records, or student-generated content if the disclosure is made under any of the following circumstances:

1. in furtherance of school purposes of the website, online service, or app, as long as the recipient of the information uses it to improve the operability and functionality of the website, service, or app;
2. to ensure compliance with federal or state law or regulations or pursuant to a court order;
3. in response to a judicial order;
4. to protect the safety or integrity of users or others, or the security of the website, online service, or app;

5. to an entity hired by the operator to provide services for the website, online service, or app, as long as the operator contractually (a) prohibits the entity from using the student information, student records, or student-generated content for any purpose other than providing the contracted service to, or on behalf of, the operator; (b) prohibits the entity from disclosing student information, student records, or student-generated content provided by the operator to subsequent third parties; and (c) requires the entity to agree to maintain security procedures and delete any student information at a student's, parent's, or guardian's request; or
6. for a school purpose or other education or employment purpose requested by a student, parent, or guardian, as long as such student information is not used or disclosed for any other purpose.

Permissible Uses Related to Products and Services

The Act permits an operator to use student information for adaptive learning purposes or customized student learning, or to do the following:

1. maintain, support, improve, evaluate, or diagnose the operator's website, online service, or app;
2. provide recommendation engines to recommend content or services relating to school purposes or other educational or employment purposes, as long as the recommendation is not determined in whole or in part by payment or other consideration from a third party; or
3. respond to a request for information or feedback from a student, as long as the response is not determined in whole or in part by payment or other consideration from a third party.

The Act permits an operator to use de-identified student information or aggregated student information to (1) develop or improve the operator's website, online service, or app or other websites, services, or apps owned by the operator or (2) demonstrate or market the effectiveness of the operator's website, online service, or app. It also permits an operator to share aggregated or de-identified student information to improve and develop websites, online services, or apps designed for school purposes.

Prohibited Effects

The Act specifies that the above provisions may not be interpreted to do any of the following:

1. limit a law enforcement agency's ability to obtain student information, student records, or student-generated content when authorized by law or court order;
2. limit a student's, parent's, or guardian's ability to download, export, transfer, or otherwise save or maintain student information, student records, or student-generated content;
3. impose a duty on an “interactive computer service” provider to ensure compliance of third-party “information content providers” (as defined in the federal Communications Decency Act of 1996, with the act's operator prohibitions and requirements;

4. impose a duty on a seller or provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software applications to review or enforce compliance with the act's operator prohibitions and requirements regarding such software apps;
5. limit an Internet service provider from giving a student, parent, guardian or board of education the ability to connect to the Internet;
6. prohibit an operator from advertising other websites, online services, or apps used for school purposes to students' parents or guardians, as long as it does not result from the operator's use of student information, student records, or student-generated content; or
7. regulate websites, online services, or apps designed and marketed for general use by individuals, even if their account credentials are designed and marketed for school purposes.

§ 4 - SECURITY BREACHES

Security Breach Involving a Contractor

Breach of Student Information. The act requires a contractor to notify the board of education without unreasonable delay upon discovering the unauthorized release, disclosure, or acquisition (i. e., "breach") of student information, directory information, student records, or student-generated content. The contractor must do so within 30 days for a breach of student information (excluding any directory information contained) and within 60 days for a breach of directory information, student records, or student-generated content.

The act defines **"directory information"** according to federal FERPA regulations.

During the 30- and 60-day periods, the act allows the contractor to (1) determine the breach's nature and scope and the identity of the students whose student information is involved or (2) restore the reasonable integrity of the contractor's data system.

Student, Parent, and Guardian Notice. Upon receiving notice of a security breach from a contractor, the board of education must electronically notify, within 48 hours, the student and parents or guardians of the student whose information, student records, or student-generated content was compromised. The board must also post this notice on its website.

Security Breach Involving an Operator

The Act requires an operator, upon discovering a security breach of student information, student records, or student-generated content as a result of a student's use of the operator's website, online service, or app, to notify the student, parents, or guardians about the breach without unreasonable delay. As with the notice requirements for contractors, the operator must do so within 30 days for breaches of student information (excluding any directory information contained) and within 60 days for breaches of directory information, student records, or student-generated content.

During the 30- and 60-day periods, the act allows the operator to (1) determine the breach's nature and scope and the identity of the students whose student information, student records, or student-generated content are involved or (2) restore the reasonable integrity of the data system.

§ 5 — STUDENT DATA PRIVACY TASK FORCE

Purpose and Charge

The act creates a 14-member task force to study student data privacy issues. The study must include an examination of the following topics:

1. when a student's parent or guardian may reasonably or appropriately request the deletion of student information, student records, or student-generated content possessed by a contractor or operator;
2. the means of providing notice to parents and guardians when a student uses an operator's website, online service, or app for instructional purposes in the classroom or as assigned by a teacher;
3. reasonable penalties for violating the act's provisions, such as restricting a contractor or operator from accessing or collecting student information, student records, or student-generated content;
4. other states' strategies that ensure that school employees, contractors, and operators are trained in data security handling, compliance, and best practices;
5. the feasibility of developing a district-wide list of approved websites, online services, and mobile apps;
6. the use of an administrative hearing process to provide legal recourse to students, parents, and guardians aggrieved by violations of this act's provisions;
7. the feasibility of creating an inventory of student information, student records, and student-generated content currently collected under state and federal law;
8. the feasibility of developing a tool kit for use by boards of education to (a) improve student data contracting practices and compliance, including a statewide template for use by districts; (b) increase school employee awareness of student data security best practices, including model training components; (c) develop district-wide lists of approved software applications and websites; and (d) increase the availability and accessibility of student data privacy information for students' parents and guardians and educators; and

Report Deadline

The Act requires the task force to submit a report on its findings and recommendations to the General Law and Education committees by January 1, 2017.

A new policy to consider, replacing the previous version in order to comply with new legislation, PA 16-189.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues

The Board of Education (Board) 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 Board, on or after October 1, 2016, 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 Board. (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 Board, 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, parent, legal guardian of a student, and the Board, 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

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues (continued)

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 Board 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 Board).
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 Board on or after October 1, 2016, that conflicts with the provisions listed above shall be void. Moreover, a contract is void if it lacks any of the above provisions. The Board will give the contractor reasonable notice to amend the contract to include the missing provisions.

Any contract entered into on and after October 1, 2016, that does not include the provisions listed above shall be void, provided the Board 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 Board 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 Board shall post such notice and the contract on the Board's Internet website.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues (continued)

The Board 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 Board 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 Board 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 Board 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 Board without unreasonable delay and in no case later than sixty (60) days from the discovery of the breach.

Note: The Board may desire to contract for more prompt notice of a breach of security.

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 Board 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

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues

Definitions (continued)

3. **"Consultant"** means a professional who provides non-instructional services, including administrative, planning, analytical, statistical, or research services to a board 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 Board.
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 Board 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

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues

Definitions (continued)

b. Is created or provided by an employee or agent of the board 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 a board of education 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. The Board, 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 site, service, or application.
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 Board, 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

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-based Issues (continued)

1. 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
2. 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 Board recognizes that an operator may:

1. Use student information (1) to maintain, support, evaluate or diagnose the operator's Internet website, online service or mobile application, or (2) for adaptive learning purposes or customized student learning.
2. Use de-identified student information (1) 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 (2) 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

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-based Issues (continued)

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 Board 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 Board, 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 Board determines that a request for directory information is not related to school purposes, the Board 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 Board to adopt regulations.

46b-56(e) Access to Records of Minors.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-based Issues

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)

Policy adopted:
cps 6/16
rev 9/16

3520.13
Form

_____ PUBLIC SCHOOLS
_____, Connecticut

STAFF REQUEST FOR APPROVAL OF TECHNOLOGY RESOURCES

Before use in the classroom, use with students, or administrative use, all online learning resources, online applications, digital subscription services, and other programs or technology applications requiring the user to accept terms of services or a user agreement must be approved by the _____ *(Technology Coordinator/Principal)*

To request to use such an online resource or technology application other than a District-approved resource, please complete and submit the following form.

Name: _____
Position: _____ *(example: teacher)*
Date:_____

If the resource will be used by students, which grade(s)?: _____

1. Give name and description of the technology resource you are requesting to use. If you are requesting an online resource, please include a link to the resource.

   _____
   _____
   _____

2. Describe how you plan to use the requested resource. What information, if any, will be shared? Who will have access to the resource? If for use by students, will students need to sign up for an account or download an application? Is parental permission required by the application before use by a student?

   _____
   _____
   _____
   _____

For Office Use Only

☐ Approved for use

- ☐ Additional parental notification and permission required.
- ☐ No additional notifications or permissions required.

☐ Not approved for use at this time

- ☐ Reason: _____