Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues

The Bethany 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, 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 continue 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 services contractor.)
2. A description of the means by which the Board may request the deletion of any student information, student records, or student-generated content in the possession of the contractor that is not a) otherwise prohibited from deletion or required to be retained under state or federal law, or b) stored as a copy of a disaster recovery storage system and that is i) inaccessible to the public, and ii) unable to be used in the normal course of business by the contractor, provided the Board may request the deletion of any such student information, student records or student-generated content if such copy has been used by the operator to repopulate data following a disaster recovery.
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/legal guardian of a student may review personally identifiable information (PII) contained in the student's records, 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 record, student information, and student-generated content.
6. A description of the procedures that a contractor will follow for notifying the Board, in compliance with Connecticut General Statutes Section 10-234dd, when there has been an unauthorized release, disclosure, or acquisition of student information, student records, or student-generated content.
7. A statement that a student's records, student information, or student-generated content shall not be retained or available to the contractor upon expiration of the contract between the contractor and the Board except a student, parent, or legal guardian of a student may choose to independently establish or maintain an electronic account with the contractor after the expiration of such contract for the purpose of storing student-generated content.

8. A statement that the contractor and the Board shall ensure compliance with the federal Family Educational Rights and Privacy Act, 20 U.S.C. 1232g (FERPA).
9. A statement that Connecticut laws shall govern the contract and the rights and duties of all parties to the contract including the 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.

The Board of Education may use the uniform student data privacy terms-of-service agreement addendum, developed by the Commission for Educational Technology (CET), in contracts entered into pursuant to C.G.S. 10-234bb. Such amendment shall conform to the requirements for a contract listed above.

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

Any contract or a terms of service agreement addendum that does not include the provisions listed above shall be void provided the Superintendent or designee has given reasonable notice to the contractor and the contractor has failed within a reasonable time to amend the contract or the terms of service agreement addendum to include the required provisions.

The Superintendent or designee shall maintain and update, as necessary, a website with information relating to all contracts entered into pursuant to this policy. Not later than five (5) business days after executing a contract pursuant to this policy, the Superintendent or designee shall post notice of such contract on the District's website. The notice shall include the contract and:

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.

On or before September 1st annually, the Superintendent or designee shall electronically notify students and the parents/guardians of students of the address of the Internet website described in this policy.

The Superintendent or designee and a contractor may include in any contract executed pursuant to this policy, a student data privacy terms of service agreement addendum, previously described, to satisfy the requirements of this policy.

The Board is not required to enter into a contract pursuant to this policy if the use of an Internet website, online service, or mobile application operated by a consultant or an operator is unique and necessary to implement a child's individualized education program or plan pursuant to Section 504 of the Rehabilitation Act of 1973, as amended from time to time, and such Internet website, online service or mobile application is unable to comply with the provisions of this policy, provided:

1. such Internet website, online service, or mobile application complies with the FERPA, as amended from time to time, and the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended from time to time.
2. The Board can provide evidence that it has made a reasonable effort to:
    a. enter into a contract with such consultant or operator to use such Internet website, online service or mobile application, and
    b. find an equivalent Internet website, online service, or mobile application operated by a consultant or an operator that complies with the provisions of this section.
3. The consultant or operator complies with the provisions of Section 10-234cc, as amended for such use, and
4. The parent/legal guardian of such child and, in the case of a child with an individualized education program, a member of the planning and placement team, sign an agreement that
    a. Acknowledges such parent/legal guardian is aware that such Internet website, online service or mobile application is unable to comply with the provisions of this policy, and
    b. Authorizes the use of such Internet website, online service or mobile application

The Superintendent or designee shall, upon request of a child's parent/legal guardian, provide the evidence described above to such parent/legal guardian.

The Board expects that an operator shall implement and maintain security procedures and practices that meet or exceed industry standards and that are designed to protect student information, student records, and student-generated content from unauthorized access, destruction use, modification, and disclosure; and delete any student information, student records or student-generated content within a reasonable amount of time if a student, parent/guardian or Board requests deletion of such student information, student records or student-generated content unless:

1. State or federal law prohibits such deletion or otherwise requires the retention of such student information, student records or student-generated content, or
2. A copy of such student information, student records, or student-generated content is in the possession of the operator as part of a disaster recovery storage system and is inaccessible to the public and unable to be used in the normal course of business by the operator, provided such student, parent/legal guardian of a student or the Board may request the deletion of any such student information, student records or student-generated content if such copy is used by the operator to repopulate accessible data following a disaster recovery.

The Superintendent or designee will utilize the written guidance developed by the Department of Education in consultation with the Commission for Educational Technology concerning the implementation of FERPA and the laws relating to student data privacy. Such written guidance includes a plain language explanation of how such student data privacy laws are to be implemented, information about the uniform student data privacy terms-of-service agreement addendum, and how such addendum may be incorporated into contracts executed pursuant to Section 10-234bb, as amended.

Notice of Breach of Security/Data Breacher

Upon notice of a breach of security by a contractor, the Board shall, not later than two (2) business days after receipt of such notice, notify the students and the parents or legal guardians of the students whose student information, student records, or student-generated content was involved in such breach. The Superintendent or designee 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 Superintendent or designee 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 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.
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 Connecticut 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 information that has been altered to prevent the identification of an individual student.
6. **Eligible student** means a student who has reached eighteen (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** mean:

   any information directly related to a student that is maintained by the 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 do 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.

b. Is created or provided by an employee or agent of the Board, 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 school District or aid in the administration of school activities, including, but not limited to, instruction in the classroom, administrative activities, and collaboration between students, school personnel, or parents or 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 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 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.
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.
4. Disclose student information unless the disclosure is made:
    a. in furtherance of school purposes of the Internet website, online service, or online 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 service provider comply with this policy.

The Board 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; 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 U.S.C. 230, as amended from time to time;
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 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 Superintendent or designee, 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 Superintendent or designee determines that a request for directory information is not related to school purposes, the District shall not disclose such directory information.

Legal References: Connecticut General Statutes § 1-19(b)(11)

Connecticut General Statutes § 7-109

Connecticut General Statutes § 10-15b

Connecticut General Statutes § 10-209

Connecticut General Statutes § 10-234aa

Connecticut General Statutes § 10-234bb, as amended

Connecticut General Statutes § 10-234cc

Connecticut General Statutes § 10-234dd, as amended

Connecticut General Statutes § 11-8a

Connecticut General Statutes § 11-8b

Connecticut General Statutes § 46b-56(e)

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

Public Act 16-189

Public Act 17-200

Public Act 18-125

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.)

Department of Education 34 C.F.R. Part 99 (May 9, 1980, 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education 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: April 13, 2016
Policy revised: January 11, 2017
Policy revised: December 13, 2017
Policy revised: December 12, 2018
Policy revised: December 8, 2021
Policy revised: October 8, 2025

Source: CABE