POLICY SUB-COMMITTEE MEETING
Regular Meeting
Griswold Board of Education
Superintendent's Office
211 Slater Avenue
Griswold, CT 06351

TUESDAY,
October 8th, 2024
5:00 PM

1. Call to Order

2. Approval of the Minutes—September 10th, 2024

3. Review, Discussion, and Possible Action on New Policy 3171.1—Business and Non-Instructional Operations—Non-Lapsing Fund (Non-Regional School Districts)

4. Review, Discussion, and Possible Action to Revise Bylaw 9324—Advance Delivery of Meeting Materials

5. Review, Discussion, and Possible Action to Revise Policy 4112.5/4212.5—Personnel—Certified/Non-Certified—Security Check/Fingerprinting

6. Review, Discussion, and Possible Action to Revise Regulation 4112.5/4212.5—Personnel—Certified/Non-Certified—Security Check/Fingerprinting

7. Review, Discussion, and Possible Action to Approve New Policy 3542.31 Business/Non-Instructional Operations—Free or Reduced Price Lunches—Participation in the National School Lunch Program

8. Review, Discussion, and Possible Action to Approve New Policy 3516.11 Business/Non-Instructional Operations—Hazardous Materials Communication

9. Review, Discussion, and Possible Action to Approve New Policy 3326.3—Business/Non Instructional Operations—Board of Education Credit Card

10. Review, Discussion, and Possible Action to Revise Bylaw 9311 Formulation, Adoption, and Amendments of Policies

11. Review, Discussion, and Possible Action to Revise Bylaw 9130 Committees

12. Next Meeting: Tuesday, November 12th, 2024

13. Adjourn

POLICY SUB-COMMITTEE MEETING
GRISWOLD BOARD OF EDUCATION

TUESDAY,
SEPTEMBER 10th, 2024

DRAFT

1. A regular meeting of the Griswold Board of Education's Policy Subcommittee took place on Tuesday, September 10th, 2024, at Griswold Middle School, Superintendent's office, 211 Slater Avenue, Griswold, Connecticut. The Policy Subcommittee meeting was called to order at 5:00 PM by Yvonne Palasky, Chair of the Policy Subcommittee.

PRESENT Yvonne Palasky, GPS Policy Subcommittee Chair; Mary Beth Malin and Jaimee O'Neill-Eaton, GPS Policy Subcommittee Members.

ALSO PRESENT Sean McKenna, GPS Superintendent of Schools; and Deb Martin, GPS Director of Fiscal & Personnel Services.

ABSENT

2. Approval of the Regular Meeting Minutes—May 7th, 2024

MOTION
By Mary Beth Malin
Seconded by Jaimee O'Neill-Eaton
To approve the regular meeting minutes of May 7th, 2024, as presented.
Motion unanimously carried.

3. Approval of the Special Meeting Minutes – September 3rd, 2024

MOTION
By Mary Beth Malin
Seconded by Jaimee O'Neill-Eaton
To approve the special meeting minutes of September 3rd, 2024, as presented.
Motion unanimously carried.

4. Review, Discussion, and Possible Action on New Policy 0050—Mission-Goals-Objectives—Code of Ethics

MOTION
By Jaimee O'Neill-Eaton
Seconded by Mary Beth Malin
To bring forward new policy 0050, as discussed, to the full Board of Education.
Motion unanimously carried.

5. Review/Discussion, and Possible Action on New Bylaw of the Board 9325.5 – Requests for Information by Board Members

MOTION

By Jaimee O'Neill-Eaton
Seconded by Mary Beth Malin
To bring forward new bylaw of the Board 9325.5, as discussed, to the full Board of Education.
Motion unanimously carried.

6. Review/Discussion, and Possible Action on New Policy 3171.1 – Business and Non-Instructional Operations – Non-Lapsing Fund (Non-Regional School Districts)

MOTION

By Jaimee O'Neill-Eaton
Seconded by Mary Beth Malin
To table this new policy until the next Policy subcommittee meeting.
Motion unanimously carried.

7. Review, Discussion, and Possible Action on New Policy 0100 – Mission – Goals – Objectives – Mission Statement

MOTION

By Mary Beth Malin
Jaimee O'Neill-Eaton
To move forward new policy 0100, as discussed, to the full Board of Education.
Motion unanimously carried.

8. Review, Discussion, and Possible Action on New Policy 0521.2 – Mission – Goals – Objectives – Nondiscrimination – Commitment to Religious Neutrality (Prayer in Schools)

MOTION

By Mary Beth Malin
Seconded by Jaimee O'Neill-Eaton
To move forward new policy 0521.2, as discussed, to the full Board of Education.
Motion unanimously carried.

9. Next Meeting: Tuesday, October 8th, 2024 – The Policy subcommittee will hold their next regular meeting on Tuesday, October 8th, 2024, at 5 PM.

10. Adjourn

MOTION

By Mary Beth Malin
Seconded by Jaimee O'Neill-Eaton
To adjourn the Policy subcommittee meeting at 5:50 PM.
Motion unanimously carried.

Minutes prepared by: Sean McKenna/Robin Drobiak

NON-LAPSING ACCOUNT/EDUCATION FUND

(BACKGROUND INFORMATION FOR POLICY REVIEW COMMITTEE)

***2024 Legislative Update Impacting Board of Education Non-Lapsing Account/Education Fund**

Prior to the passage of Public Act 24-45 An Act Concerning Education Mandate Relief, School Discipline, and Disconnected Youth, Section 7 state law (Connecticut General Statutes §10-248a) allowed a town board of finance (or the board of selectmen in a town with no board of finance, or the authority otherwise making budget appropriations for the school district) to deposit unexpended funds from the education budget into a non-lapsing account.

Beginning with the **2023-2024 fiscal year,** Section 7 of Public Act 24-45 will allow the local board of education to make this deposit. Current restrictions in the law will continue to apply: 1) the deposited amount cannot exceed 2% of the prior fiscal year's education budget; 2) any expenditures from this account are only made for educational purposes; and 3) any expenditure must be authorized by the town's board of education. However, this new provision will allow local boards of education to decide how much, if any, to place into such an account (up to the 2% cap) or create one if one does not exist. Previously, local boards of education were reliant upon the willingness of a town's fiscal authority to create such an account (and then make any deposits into it), and often, a town's fiscal authority would refrain from doing so, since any unexpended monies would otherwise revert back to the town at the end of the fiscal year.

Regional Boards of Education: Authority to Use Reserve Funds for any Educational Purpose

Prior to the same Act, Section 8, state law (Connecticut General Statutes §10-51(d)(2) allowed regional boards of education to create reserve funds for "capital and non-recurring expenditures," to be financed by appropriated funds and year end surplus operating (budget) funds. **Beginning with the 2023-2024 fiscal year,** Section 8 of Public Act 24-45 will allow *regional boards of education* to create (and expend monies from) these funds *for any "educational expenditure,"* not just capital projects/improvements and equipment purchases. The Act renames the account "**the reserve fund for educational expenditures**" instead of the former "reserve fund for capital and nonrecurring expenditures." The other current restrictions for these reserve funds will remain in effect (for example, that such accounts be created by a majority vote of the regional board of education's members, the aggregate amount of annual appropriations and supplemental appropriations from the surplus by the regional district to the fund cannot exceed 2% of the annual district budget for the fiscal year). However, this revision provides an additional tool for regional school districts to consider when determining what to do with any surplus, and whether to 1) reduce the budget assessments to their member towns for the next year, or 2) use the surplus for educational purposes in the future via a deposit into a reserve fund.

Policy Implications

A revision to policy, #3171.1, taking into consideration 2024's Public Act 24-45, Section 7, "Non-Lapsing Education Fund," and Section 8 "Reserve Fund for Educational Expenditures" follows for consideration. This is considered an optional policy for inclusion in a district's policy manual.

A "Memorandum of Agreement" between the board of education and the board of finance is no longer required.

April 2015
Revised July 2019
Revised July 2024

An optional policy to consider.

Business and Non-Instructional Operations

Non-Lapsing Education Fund (Non-Regional School Districts)

The _____ Board of Education (Board) may ~~request the town's Board of Finance~~ deposit into a non-lapsing account any unexpended funds from the Board's prior fiscal year general operating budget, provided such deposited amount does not exceed two percent (2%) of the total budgeted appropriation for education for such prior fiscal year pursuant to C.G.S. 10-248a.

Any expenditure from the Non-Lapsing Education Fund shall be authorized solely by the Board of Education. Each expenditure from such account shall be made only for educational purposes and under the following conditions:

(1) such deposited amount does not exceed two percent (2%) of the total budgeted appropriation for education for such prior fiscal year;

(2) each expenditure from such account shall be made only for educational purposes; and

(3) each such expenditure shall be authorized by the _____ Board of Education.

The Board of ~~Finance~~ Education shall create the non-lapsing account and be responsible for the accounting of the funds in accordance with Governmental Accounting Standards and Generally Accepted Accounting Principles (GAAP). The account shall be subject to the annual audit as required by State statute. The Board of Education shall review the fund balance on an annual basis.

Reserve Fund for ~~Capital and Nonrecurring~~ Educational Expenditures (Regional School Districts)

The Regional Board of Education (Board), by a majority vote of its members, may create a reserve fund for ~~capital and nonrecurring~~ educational expenditures. Such fund shall be termed "reserve fund for ~~capital and nonrecurring~~ educational expenditures." The aggregate amount of annual and supplemental appropriations by a district to such fund shall not exceed two percent (2%) of the annual district budget for such fiscal year.

Annual appropriations to such fund shall be included in the share of net expenses to be paid by each member town. Supplemental appropriations to such fund may be made from estimated fiscal year end surplus in operating funds. Interest and investment earnings received with respect to amounts held in the fund shall be credited to such fund.

The Board shall annually submit a complete and detailed report of the condition of such fund to the member towns. Upon the recommendation and approval by the Board, any part or the whole of such fund may be used for ~~capital and nonrecurring~~ educational expenditures ~~but such use shall be restricted to the funding of all or part of the planning, construction, reconstruction or acquisition of any specific capital improvement or the acquisition of any specific item of equipment~~.

Business and Non-Instructional Operations

Non-Lapsing Education Fund (Non-Regional School Districts) (continued)

Such fund may be discontinued, after the recommendation and approval by the Board, and any amounts held in the fund shall be transferred to the general fund of the District.

Legal Reference: Connecticut General Statutes

10-51 (d) (2) Fiscal year. Budget. Payments by member towns; adjustments to payments. Investment of funds. Temporary borrowing. Reserve funds. (as amended by PA 21-2, JSS, Section 363)

10-222 Appropriations and budget

10-248a Unexpended education funds account (as amended by PA 19-117, Section 285)

Public Act 24-45 An Act Concerning Education Mandate Relief, School Discipline and Disconnected Youth (Sections 7-8)

Policy adopted:
cps 4/15
rev 7/19
rev 10/21
rev 7/24

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

Bylaws of the Board

Advance Delivery of Meeting Materials

The Board meeting materials shall be disseminated as follows:

1. The complete Board of Education agenda and the appropriate materials pertaining thereto shall be sent to each Board member.

   The agenda will be available to the public at the Central Office and the district website after 3:00 P.M. on Fridays preceding each regular Board of Education meeting. An agenda will also be available to each member of the press on Friday afternoons.

2. Electronic copies of the agenda shall be forwarded to presidents of each bargaining unit.

(cf. 9323 - Construction/Posting of Agenda)

Bylaw adopted by the Board: May 28, 2013

GRISWOLD PUBLIC SCHOOLS
Griswold, Connecticut

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

In order to create a safe and orderly environment for students, all offers of employment will be conditional upon the successful outcome of a criminal record check. In addition, any person applying for employment with the Board shall submit to a record check of the Department of Children and Families Child Abuse and Neglect Registry before the person may be hired.

Note: Applicants for all positions, certified or non-certified must submit to a check of Department of Children and Families Child Abuse and Neglect Registry.

Applicants, as required, shall make disclosures containing (1) current and past employers' contact information; (2) authorization allowing contact with such employers; and (3) statements about any past misconduct, discipline, or licensure penalties as a result of sexual misconduct or abuse allegations.

The District, prior to hiring such applicants, applicants, will (1) ensure that they complete the above stated three requirements; (2) review applicants' employment history after making a documented, good faith effort to contact previous employers for information; and (3) request any available information about applicants from SDE.

The background/reference checks shall be done in compliance with the statutory guidelines contained in Board policy #4112.51/4212.51, as ~~amended~~ updated in 2019.

District employees shall within 30 days after they are hired submit to state and national criminal checks. District students employed by the school system are exempted from this requirement.

Workers placed in a school under a public assistance employment program shall also submit to the criminal check if such individuals will have direct contact with students.

~~School nurses and nurse practitioners appointed by the Board or under contract with the Board shall also submit to a criminal history check pursuant to C.G.S. 29-17a.~~

Student teachers placed in District schools as part of completing preparation requirements for the issuance of an educator certificate, effective July 1, 2010, shall also be required to undergo the same criminal background checks already required for school employees.

A District student, employed by the District or a person employed by the Board as a teacher for a non-credit adult class or adult education activity (as defined in C.G.S. 10-67) who is not required to hold a teaching certificate, pursuant to C.G.S. 10-145b, as amended by PA 18-51, is exempt from the fingerprinting requirement.

Criminal Justice Information

Criminal Justice Information (CJI) is to be maintained in accordance with the administrative regulation pertaining to the use and disclosure of criminal justice information.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

(cf. 4112.51/4212.51 - Employment/Reference Checks)

Legal Reference: Connecticut General Statutes

10-221d Criminal history records checks of school personnel. Fingerprinting. Termination or dismissed. (as amended by PA 01-173, PA 04-181 and June 19 Special Session, PA 09-1, PA 11-93 and PA 16-67 and PA 18-51)

29-17a Criminal history checks. Procedure. Fees.

PA 16-67 An Act Concerning the Disclosure of Certain Education Personnel Records

Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, October 6, 2015.

Criminal Justice Information Services (CJIS) Security Policy, Version 5.8, June 2019.

Policy adopted: August 28, 2017
Policy Revised: November 13, 2018

GRISWOLD PUBLIC SCHOOLS
Griswold, Connecticut

CURRENT REGULATION

R4112.5(a)
4212.5

Personnel – Certified/Non-Certified

Security Check/Fingerprinting

Each person hired by the school system shall be required to submit to state and national criminal record checks. In order to process such record checks, the following procedure will be followed:

1. No later than ten calendar days after the Superintendent or his/her designee has notified job applicant of a decision to hire the applicant, or as soon thereafter as practicable, the Superintendent or his/her designee will supply the applicant with a packet containing all documents and materials necessary for the applicant to be fingerprinted by the Regional Service Center. This packet shall also contain all documents and materials necessary for the Regional Service Center to submit the completed fingerprints to the State Police Bureau of Identification for the processing of state and national criminal record checks.

2. No later than ten calendar days after the Superintendent or his/her designee has provided the successful job applicant with the fingerprinting packet, the applicant must arrange to be fingerprinted. Failure of the applicant to have his/her fingerprints taken within such ten-day period, without good cause, will be grounds for the withdrawal of the offer of employment.

3. Any person for whom criminal records checks are required to be performed pursuant to this policy must pay all fees and costs associated with the fingerprinting process and/or the submission or processing of the requests for criminal record checks.

4. Upon receipt of a criminal record check indicating a previously undisclosed conviction, the Superintendent or his/her designee will notify the affected applicant/employee in writing of the results of the record check and will provide an opportunity for the affected applicant/ employee to respond to the results of the criminal record check.

5. Decisions regarding the effect of a conviction upon an applicant/employee, whether disclosed or undisclosed by the applicant/employee, will be made on a case-by-case basis. Notwithstanding the foregoing, the falsification or omission of any information on a job application or in a job interview, including, but not limited to information concerning criminal convictions or pending criminal charges, shall be grounds for disqualification from consideration for employment or discharge from employment.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

6. Each applicant for a position involving direct student contact is required to make three disclosures to the Board for a position involving direct student contact. The applicant must:

   a. Provide the District with contact information for current and former employers if they were education employers or the employment otherwise involved contact with children. The contact information must include each employer's name, address, and telephone number.

   b. Provide a written authorization that consents to and authorizes such former employers to disclose information and related records about him or her that is requested on the SDE-designed standardized form that interviewing education employers send. The authorization also must consent to and authorize SDE to disclose information and related records to requesting education employers and release such former employers and SDE from any liability that may arise from such disclosure or release.

   c. Give a written statement about whether he or she:

      i. was the subject of an abuse or neglect or sexual misconduct investigation by any employer, state agency, or municipal police department, unless the investigation resulted in a finding that all allegations were unsubstantiated;

      ii. was disciplined or asked to resign from a job or resigned from or otherwise separated from any job while an allegation of abuse or neglect was pending or under investigation by the Department of Children and Families (DCF), or an allegation of sexual misconduct was pending or under investigation or because of an allegation substantiated by DCF of abuse or neglect or sexual misconduct or a conviction for abuse or neglect or sexual misconduct; or

      iii. had a professional or occupational license or certificate suspended or revoked or ever surrendered one while an allegation of abuse or neglect was pending or under investigation by DCF, or an investigation of sexual misconduct was pending or under investigation, or because of an allegation substantiated by DCF of abuse or sexual misconduct or a conviction for abuse or sexual misconduct.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

7. The District is prohibited from offering employment for any position involving direct student contact until the following has occurred:

   a. the applicant has complied with the above disclosure requirements;

   b. the District has reviewed, either through written or telephone communication, the applicant's employment history on the standardized form filled out by current and past employers, which current or former employers must complete and return within five business days of receipt; and

   c. the District has requested information from SDE about the applicant's eligibility status for a position requiring a certificate, authorization, or permit; previous disciplinary action for a substantiated finding of abuse or neglect or sexual misconduct; and notice of a criminal conviction or pending criminal charges against the applicant.

8. A good faith effort to reach an applicant's current and previous employers shall be made. A "good faith effort" is one requiring no more than three phone calls on three separate days.

9. The District may request additional information from an applicant's current or former employers relating to any response the applicant listed on the standardized SDE form, to which the applicant must respond within five business days of receipt. Immunity is provided from criminal and civil liability to any employer who provides such information, as well as to SDE, as long as the information supplied is not knowingly false.

10. The information available to the Board from SDE about an applicant may include:

    a. any information about the applicant's eligibility for employment with such education employer in a position that requires a certificate, authorization, or permit;

    b. whether SDE knows if the applicant was disciplined for a finding of abuse or neglect or sexual misconduct, and any information related to the finding; and

    c. whether SDE has been notified that the applicant has been convicted of a crime or of pending criminal charges against the applicant and any information about such charges.

11. Applicants for substitute teaching positions must also fulfill the disclosure requirements as listed above. The District will also request information from the applicant's prior employers and SDE (in the same manner required for other applicants).

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

12. Adult education teachers and substitute teachers, if they are continuously employed by the district, do not have to be re-fingerprinted after fulfilling the initial requirement.

13. The District shall maintain a list of individuals suitable to work as substitute teachers. Only those on the list may be hired as substitute teachers. An individual remains on the list as long as (1) he or she is continuously employed by the District as a substitute teacher and (2) District does not have any knowledge that would cause the person to be removed from the list.

14. School nurses and nurse practitioners appointed by the Board or under contract with the Board shall also submit to a criminal history check pursuant to C.G.S. 29-17a.

15. Student teachers placed in District schools as part of completing preparation requirements for the issuance of an educator certificate shall also submit to a criminal history check. The criminal history check shall be done prior to being placed in a school for clinical experiences such as field experiences, student teaching or internship. Candidates are required to be fingerprinted at one of the RESCs and not through local police stations or the school district. The District is required to notify the State Board of Education if notice is received that a student teacher has been convicted of a crime.

16. Each applicant for a certified position must submit to a records check of the Department of Children and Families (DCF) Child Abuse and Neglect Registry established pursuant to C.G.S. 17a-101k before the applicant may be hired. The Superintendent or his/her designee shall request the required records check of DCF in accordance with the procedures established by DCF.

17. Each applicant for a non-certified position must submit to a records check of the Department of Children and Families (DCF) Child Abuse and Neglect Registry established pursuant to C.G.S. 17a-101k before the applicant may be hired. The Superintendent or his/her designee shall request the required records check of DCF in accordance with the procedures established by DCF.

18. Contractors that apply for positions involving direct student contact are required to perform the checks on their employees who would fill such positions. These checks are similar to the ones the District must perform on applicants.

    a. A contractor's employee must fulfill the three disclosure requirements that a regular, direct applicant for such a position must fulfill.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

b. The contractor must contact any current or former employers that were education employers and request, by telephone or in writing, any information about whether there was a finding of abuse or neglect or sexual misconduct against the employee, and which the employer must report if there is one.

c. Should the contractor receive any information indicating such a finding or otherwise has knowledge of one, he or she must immediately forward, either by telephone or in writing, the information to the District.

d. The District must determine whether the employee may work in a position involving direct student contact at any of its schools.

e. It is not considered a breach of contract for the District to determine that the contractor's employee is forbidden to work under any such contract in such a position.

19. The District shall notify SDE when it receives information that applicants or employees have been disciplined for a finding of abuse or sexual misconduct.

20. The District is required to provide upon request, to any other education employer or to the Commissioner of Education, information it may have about a finding of abuse or sexual misconduct for someone being vetted for hire as a direct employee of the Board or a contractor's employee.

21. The Board is prohibited from entering into any collective bargaining agreement, employment contract, resignation or termination agreement, severance agreement, or any other agreement or take any action that results in any of the following outcomes:

a. has the effect of suppressing information about an investigation of a report of suspected abuse or neglect or sexual misconduct by a current or former employee;

b. affects the education employer's ability to report suspected abuse or neglect or sexual misconduct to appropriate authorities; or

c. requires the district to expunge information about an allegation or finding of suspected abuse or neglect or sexual misconduct from any documents it maintains, unless after investigation the allegation is dismissed or found to be false.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

22. The District may employ or contract with an applicant for up to 90 days while awaiting the complete review of their application information, as long as the following has occurred:

    a. the applicant has submitted to the District the three required disclosures,

    b. the District has no information about the applicant that would disqualify him or her from employment, and

    c. the applicant affirms that he or she is not disqualified from employment with the education employer.

23. Applicants who knowingly provide false information or knowingly fail to disclose information that is statutorily required to the District is subject to discipline by the District. Such discipline may include denial of employment or termination of a certified employee's contract.

Criminal Justice Information*

Policies #4112.5/4212.5 and #4112.51/4212.51 and applicable law require applicants for employment in the District to submit to state and national criminal record checks. All results for such background checks and accompanying information is considered "Criminal Justice Information (CJI)." Such information is to be maintained, used and disclosed in compliance with this administrative regulation. These regulations apply to all CJI that the District possesses or controls in any form or format, including CJI contained in correspondence, documentation or reports of the District.

Definitions

Criminal Justice Information (CJI) means the results of any state or federal criminal record checks of an applicant for employment in the district, volunteer, employee, or contractor and all copies thereof.

Criminal Justice Information Officer (CJI Officer) means the individual appointed by the Superintendent to be responsible for the use, disclosure, and safeguarding of CJI in the District. This individual serves as the District's primary point of contact for CJI matters and these regulations.

Permitted Individual means an individual designated by the Superintendent, or his/her designee, who may access CJI. Such individuals may include, but are not limited to, human resources personnel, and certain administrative staff.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

Request and Use of Criminal Justice Information

An employee, contractor, applicant, volunteer, will be asked by the District for CJI as permitted or required by applicable policy and/or law.

The Superintendent or his/her designee shall designate those individuals who will be considered "Permitted Individuals" for purposes of these regulations. CJI may not be accessed by any other member of the District staff or be used for any reason without obtaining prior written approval from the CJI Officer. CJI used by the "Permitted Individual" is limited to that permitted or required by law or District policy.

"Permitted Individuals" must satisfy applicable legal screening requirements prior to access to CJI, including the following:

1. Permitted Individuals who are Connecticut residents shall be screened by the District through a Connecticut and national fingerprint-based record check after designations as a Permitted Individual.

2. Permitted Individuals who are not Connecticut residents shall be subject to a District state and national fingerprint-based record check and follow FBI guidance pertaining to additional screening requirements.

The Connecticut Department of Emergency Services and Public Protection may be consulted by the CJI Officer pertaining to the execution of the above cited screening requirements.

A Permitted Individual's access to CJI may be terminated with or without cause at the discretion of the Superintendent, CJI Officer, or their respective designees. Upon termination of the Permitted Individual's employment in or contract with the District, such individual's access to CJI is to be immediately terminated. Reassignment or modification of a Permitted Individual's professional responsibilities is considered cause to reconsider CJI access.

Maintenance and Safeguarding of Criminal Justice Information (CJI)

The District will designate the locations, files and information systems where CJI is to be maintained. These controlled areas, locked when unattended, are limited to Permitted Individuals and other authorized personnel. If not possible to reasonably restrict access, all CJI is to be maintained in encrypted format in a manner consistent with legal requirements and industry standards.

The written approval of the CJI Officer is required in order to remove CJI from a controlled area. The CJI Officer must develop a protocol to ensure the protection of CJI while being transported and while out of the controlled area.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

Maintenance and Safeguarding of Criminal Justice information (CJI) (continued)

CJI that is maintained in paper format must be kept in a physically secure location, with a posted notice of restricted access to such records. An access log or sign-in sheet is to be used to record access to paper records.

The Criminal Justice Information Services (CJIS) Security Policy contains safeguards for CJI records maintained in electronic format which the District shall comply. These safeguards include, but are not limited to, maintaining CJI on secure electronic systems and media; positioning information systems in a manner to prevent unauthorized individuals access and viewing CJI; storing electronic media containing CJI in a secure location; instituting access controls to limit access to Permitted Individuals; validating and authenticating information system users accessing CJI; developing protocols for configuration management and providing necessary access for system modifications and maintenance; providing the capability to detect and protect against threats to the integrity of CJI; developing parameters for auditing electronic systems containing CJI; and instituting media protection policies and procedures.

Disclosure of CJI by Permitted Individuals

CJI may be disclosed by Permitted Individuals to (1) District staff upon written approval of the Superintendent, CJI Officer or their respective designees when such disclosure is viewed as reasonably necessary for the performance of District function or policy or consistent with applicable law; (2) third-party individuals/entities when such disclosure has been approved by the Superintendent or CJI Officer or their respective designees, when consistent with applicable law; or as otherwise required or permitted by law. All such disclosures shall be logged.

Security Incident Response

"Security Incident" is the actual or suspected acquisition, access, use, or disclosure of CJI in a manner not permitted by these regulations or applicable law. A Security Incident must be reported immediately to the CJI Officer, who will investigate, collect relevant evidence and respond to all such incidents.

The CJI Officer is to document each security incident including the District's response, steps taken to mitigate harm to the affected individuals and changes, as necessary to District policies and procedures to avoid a reoccurrence of such incidents.

Security incidents are to be reported in writing to the District, regarding an individual's CJI that may have been accessed, acquired or disclosed during the Security Incident. Affected individuals and/or appropriate government agencies will be notified by the District as required by law or as the District determines appropriate.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

Record Retention, Disposal and Destruction of CJI

CJI shall be maintained by the District in conformity with applicable record retention laws. Records containing CJI shall be stored for extended periods only if they are key elements for the integrity and/or utility of case files and/or criminal record files. Any audit records and transaction logs are to be maintained for one year. All records containing CJI are to be destroyed when the District is no longer required to keep CJI on file.

CJI containing paper records shall be disposed of as to make them unreadable and unable to be reconstructed, by shredding or incineration of such records. Electronic media containing CJI shall be destroyed utilizing a method that renders the CJI unreadable, indecipherable or unable to be reconstructed. Media destruction is to be done only by authorized personnel and witnessed and the method used documented.

Training

District staff with access to CJI shall initially be trained in the use, disclosure and safeguarding of such information and no less than biennially after the initial training.

(cf. 4112.51/4212.51 - Employment/Reference Checks)

Legal Reference: Connecticut General Statutes

10-221d Criminal history records checks of school personnel. Fingerprinting. Termination or dismissed. (as amended by PA 01-173, PA 04-181, June 19 Special Session, PA 09-1, PA 11-93 and PA 16-67)

17a-101k Registry of findings of abuse or neglect of children maintained by Commissioner of Children and Families. Notice of finding of abuse or neglect of child. Appeal of finding. Hearing procedure. Appeal after hearing. Confidentiality. Regulations.

29-17a Criminal history checks. Procedure. Fees.

PA 16-67 An Act Concerning the Disclosure of Certain Education Personnel Records.

PA 16-83 An Act Concerning Fair Chance Employment

Personnel – Certified/Non-Certified

Security Check/Fingerprinting (continued)

Legal Reference: Connecticut General Statutes (continued)

Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, October 6, 2015.

*This section of the administrative regulation pertaining to Criminal Justice Information (CJI) is based upon information originally developed by the law firm of Shipman and Goodwin.

Regulation approved: August 28, 2017

GRISWOLD PUBLIC SCHOOLS
Griswold, Connecticut

A new model regulation to consider, to fully comply with the procedures mandated through the Criminal Justice Information Services Security Policy,

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction

The following administrative regulations are developed to ensure Criminal Justice Information compliance:

Relevant Acronym Key

CJI/CJIS	**Criminal Justice Information/Services**
CJA	**Criminal Justice Agency**
CSA	**CJIS Systems Agencies**
CSO	**CJIS Systems Officer**
CGA	**Contracting Government Agency**
AC	**Agency Coordinator**
CSA ISO	**CJIS Systems Agency Information Security Officer**
LASO	**Local Agency Security Officer**
FBI CJIS ISO	**FBI CJIS Division Information Security Officer**
CJI	**Criminal Justice Information**
CHRI	**Criminal History Record Information**
PII	**Personally Identifiable Information**
COLLECT CJBAU	**C**T **O**n-**L**ine **L**aw **E**nforcement **C**ommunications **T**eleprocessing **C**riminal **J**ustice **B**usiness **A**pplications **U**nit

Purpose

This policy is applicable to any fingerprint-based state and national criminal history record check made for non-criminal justice purposes and requested under applicable federal authority and/or state statute authorizing such checks for hiring personnel for employment in the Griswold School District.

The following policies were developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. While the Griswold School District may complement CJIS policy with local requirements, CJIS policy shall always be the minimum standard. The local policy may augment or increase the standards but shall not detract from the CJIS Security Policy Standards.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Criminal Justice Information (CJI) and Criminal History Record Information (CHRI)

CJI is the term used to refer to all of the FBI CJIS-provided data necessary for law enforcement and civil agencies to perform their missions, including, but not limited to, biometric, identity history, biographic, property, and case/incident history data.

CHRI is a subset of CJI and is considered interchangeable for purposes of this document. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outed below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI

Requesting CHRI Checks

Fingerprint-based CHRI checks will only be conducted as authorized by the FBI and the Connecticut Department of Emergency Services and Public Protection – COLLECT CJBAU, in accordance with all applicable state and federal rules and regulations.

If an applicant or employee is required to submit to a fingerprint-based state and national criminal history record check, they shall be informed of this requirement and instructed on how to comply with the law. Such instructions will include information on the procedure for submitting fingerprints. In addition, the applicant or employee will be provided with all information needed to successfully register for a fingerprinting appointment.

Acceptable Use of CHRI

All CHRI is subject to strict state and federal rules and regulations. CHRI is used only for the official purpose for which it was requested, and CHRI cannot be shared with other entities for any purpose, including subsequent hiring determinations. All receiving entities are subject to audit by the COLLECT CJBAU (Connecticut On-Line Law Enforcement Communications Teleprocessing/Criminal Justice Business Applications Unit) and the FBI, and failure to comply with such rules and regulations could lead to sanctions. Furthermore, the Griwold School District and the employee responsible for overseeing CJI can be charged with federal and state crimes for the willful, unauthorized disclosure of CHRI.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Personnel Training

An informed review of a criminal record requires training. Accordingly, all personnel authorized to receive and/or review CHRI for the Griswold School District will review and become familiar with educational and relevant training materials regarding CHRI laws and regulations made available by the appropriate agencies.

In addition to the above, all personnel authorized to receive and/or review CHRI must undergo Security Awareness Training on a biennial basis. This training will be accomplished using the training provided by CJIS Online.

The Superintendent or his/her/their designee will be responsible for overseeing all training programs and adherence to all training requirements.

Personnel Security (All Personnel)

All personnel requiring access to CHRI must first be deemed "Authorized Personnel" by the Superintendent or his/her/their designee. The COLLECT CJBAU will review and determine if access is appropriate. Access is denied if the individual has ever had a felony conviction of any kind, no matter when it occurred. Access may be denied if the individual has one or more recent misdemeanor convictions.

In addition to the above, an individual believed to be a fugitive from justice or having an arrest history without convictions will be reviewed to determine if access to CHRI is appropriate. The COLLECT CJBAU will take into consideration extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

Persons already having access to CHRI and who are subsequently arrested and/or convicted of a crime will:

1. Have their access to CVHRI suspended until the outcome of an arrest is determined and reviewed by the COLLECT CJBAU to determine if continued access is appropriate;
2. Have their access suspended indefinitely if a conviction results in a felony of any kind;
3. Have their access denied by the COLLECT CJBAU, where it is determined that access to CHRI by the person would not be in the public's best interest.

Support personnel, contractors, and custodial workers will be denied access to CHRI. If such persons need to be in an area (s) where CHRI is maintained or processed (at rest or in transit), they will be escorted by authorized personnel or under their supervision at all times while in the area(s). .

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Personnel Termination

The Local Agency Security Officer (LASO) shall terminate access to CHRI immediately upon notification of an individual's termination of employment.

The Griswold School District shall follow the following CHRI termination process:

1. Notification will be sent via email to the COLLECT CJBAU;
2. This is to be done within 24 hours of receiving notification of termination;
3. All keys, email accounts, and other district accounts and materials identified by the Superintendent. will be obtained/disabled from the user within 24 hours.

Adverse Decisions Based on CHRI

If inclined to make an adverse decision based on an individual's CHRI, the Griswold School District will take the following steps prior to making a final adverse determination:

1. Provide the individual the opportunity to complete or challenge the accuracy of his/her/their CHRI; and
2. Provide the individual with information on the process for updating, changing, or correcting CHRI.

A final adverse decision based on an individual's CHRI will not be made until the individual has been afforded a reasonable fifteen-day period (15) to correct or complete the CHRI.

Non-Criminal Agency Coordinator (TAC)

The Griswold School District TAC is the Superintendent or Designee and is responsible for the following:

1. Maintaining an updated Authorized Personnel List on file with the COLLECT CJBAU.
    a. Ensuring everyone included on this list must undergo the appropriate level of CJIS Security Awareness Training;
    b. Ensuring everyone included on the list has appropriate access based on job functions and a need-to-know basis.
2. Inform the COLLECT CJBAU of changes in the agency head or any relevant business information (agency name changes, mailing/physical address changes, etc.).
    a. Contact the COLLECT CJBAU immediately to update the User Agreement and, if necessary, submit the new authorization to the COLLECT CJBAU;
    b. Submit a TAC change form to the COLLECT CJBAU in the event of a change in roles.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Local Agency Security Officer (LASO)

The Griswold School District LASO is the Superintendent's Executive Assistance and is responsible for the following:

1. Identifying who is using or accessing CHRI and/or systems with access to CHRI;
2. Ensuring that personnel security screening procedures are being followed as stated in this policy.
3. Ensuring the approved and appropriate security measures are in place and working as expected.

Storage of CHRI

CHRI shall only be stored for extended periods of time when necessary to ensure the integrity and/or utility of an individual's personnel file. Administrative, technical, and physical safeguards, which comply with the most recent COLLECT CJBAU and FBI Security Policy, have been implemented to ensure the security and confidentiality of CHRI. Each individual involved in the handling of CHRI is to become familiarized with these safeguards.

In addition to the above, each individual involved in handling CHRI will strictly adhere to the policy on its storage and destruction.

Media/Physical Protection

All media containing CHRI must be protected and secured at all times. The following is established and to be implemented to ensure the appropriate security, handling, transporting, and storage of CHRI media in all forms.

Controls shall be in place to protect electronic and physical media containing CHRI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CHRI.

The District shall securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to only authorized individuals. If physical and personnel restrictions are not feasible, the data shall be encrypted per Section 5.10.1.2.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Physical Storage and Access

Physical CHRI media shall be securely stored within physically secured locations or controlled areas. A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Access to such media is restricted to authorized personnel only and shall be secured at all times when not in use or under the supervision of an authorized individual.

Only authorized personnel will have access to physically secure non-public locations. The Superintendent or his/her/their designee will maintain and keep a list of authorized personnel. Before granting access, all physical access points into the District's secure areas will be authorized. The Superintendent or his/her/their designee will implement access controls and monitor physically secure areas to protect all transmission and display mediums of CJI.

Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical, and electronic breaches.

Physical CHRI media:

1. Is to be stored within employee records when feasible or by itself when necessary.
2. Is to be maintained within a lockable filing cabinet, drawer, closet, office, safe, vault, or other secure container.

Electronic CHRI media:

1. Is to be stored on secure servers within a physically secure location when feasible.
2. (Include details on how electronic CHRI is secured.)

Destruction of CHRI

Disposal of Physical Media

Once physical CHRI media (paper/hard copies) is determined to be no longer needed by the District, it shall be destroyed and disposed of appropriately. Physical CHRI media shall be destroyed by cross-cut shredding or incineration. The Superintendent or his/her/their designee will ensure such destruction is witnessed or carried out by authorized personnel:

1. The LASO shall witness or conduct disposal
2. Cross-cut shredding will be the method of destruction used by the District.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction (continued)

Destruction of CHRI

Media Sanitization and Disposal (Disposal of Electronic Media)
Once the District determines that electronic CHRI media (data stored on computers) are no longer needed, they shall be destroyed and disposed of appropriately.

The _____ Public Schools shall choose one of the following options below to use in this policy:

Option 1: Overwriting

Overwriting involves a program writing onto the media where the file to be sanitized is located. The NCJA will sanitize the electronic CHRI by overwriting the data at least three times before disposing of or reusing the computer/device/system on which it was stored. Overwriting the CHRI data must be completed or witnessed by authorized district personnel.

Option 2: Degaussing

Degaussing is a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets are weak and cannot effectively degauss magnetic media. The NCJA will degauss the electronic CHRI prior to disposing of or reusing the computer/device/system on which the electronic CHRI was stored. Degaussing the CHRI data must be completed or witnessed by authorized district personnel. (Degaussing means neutralizing a magnetic field to erase information from a magnetic disk or other storage device.)

Option 3: Destruction

If the computer/device on which the CHRI data is stored is no longer operational, The NCJA must physically destroy the device. Destruction of the device containing physical electronic CHRI, including printouts and other media, shall be disposed of by one of the following methods:

Remote Access

The Superintendent shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access means any temporary access to an agency's information system by a user or information system communicating temporarily through an external, non-district-controlled network, such as the Internet.

The District shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The Superintendent or his/her/their designee shall control all remote access through managed access control points and may permit remote access for privileged functions only for compelling operational needs. However, this person shall document the rationale for such access in the security plan for the information system.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction

Destruction of CHRI (continued)

Remote Access (continued)

It is prohibited to use publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to, hotel business center computers, convention center computers, public library computers, and public kiosk computers.

Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. A personal device includes portable technology like a camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards, mobile wireless devices, or any personal desktop computer. When bringing your own devices are authorized, they shall be controlled using the requirements in Section 5.13 of the CJIS Security Policy.

Disciplinary

If an individual employed by the _____Public School District has misused or is currently misusing CHRI, the following requirements will be adhered to:

1. Using CHRI for any purpose other than what is allowed by state statute or Federal code is considered misuse.
2. **The specific steps the District will take in the event intentional misuse is discovered.
3. Misuse of CHRI can result in loss of access to CHRI, loss of employment, and/or criminal prosecution.
4. Misuse of CHRI shall be reported to the State.

**(CABE's Policy Department recommends consulting with the Board attorney regarding item #2 and a general review of the Disciplinary section of this policy.)

Incident Response

The security of information and systems in general, and of CHRI in particular, is a top priority for the _____ Public School district. Therefore, the District has established appropriate operational incident response procedures for instances of an information security breach. It is each individual's responsibility to adhere to established security guidelines and policies and to be attentive to situations and incidents that pose risks to security. Furthermore, it is each individual's responsibility to immediately report potential or actual security incidents to minimize any breach of security or loss of information.

Personnel – Certified/Non-Certified

Security Check/Fingerprinting/Criminal Justice Information

CHRI Retention and Destruction

Incident Response (continued)

The following security incident handling procedures must be followed by each individual:

1. All incidents will be reported directly to the LASO.
2. If any records are stolen, the incident will also be reported to appropriate authorities.
3. Once the cause of the breach has been determined, disciplinary measures will be taken in accordance with the disciplinary policy of the District

In addition to the above, the LASO shall report all security-related incidents to the COLLECT CJBAU within 24 hours.

All District personnel with access to FBI and/or COLLECT CJBAU CHRI have a duty to protect the system and related systems from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the information. All existing laws, District regulations, and policies apply, including those that may apply to personal conduct. Misuse or failure to secure any information resources may result in temporary or permanent restriction of all privileges up to employment termination.

The Superintendent shall ensure that all staff members are aware of this policy and that those responsible for implementation and oversight receive adequate training and updates.

(cf. 4112.51/4212.51 - Employment/Reference Checks)

Legal Reference: Connecticut General Statutes

10-221d Criminal history records checks of school personnel. Fingerprinting. Termination or dismissed. (as amended by PA 01-173, PA 04-181, June 19 Special Session, PA 09-1, PA 11-93, PA 16-67 and PA 18-51, and PA 19-91)
17a-101k Registry of findings of abuse or neglect of children maintained by Commissioner of Children and Families. Notice of finding of abuse or neglect of child. Appeal of finding. Hearing procedure. Appeal after hearing. Confidentiality. Regulations.
29-17a Criminal history checks. Procedure. Fees.
PA 16-67 An Act Concerning the Disclosure of Certain Education Personnel Records.
PA 16-83 An Act Concerning Fair Chance Employment
Criminal Justice Information Services (CJIS) Security Plan, Version 5.8, 06/01/2019 Prepared by CJIS Information Officer Approved by CJIS Advisory Policy Board

Regulation approved:

cps 4/24

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

A recommended policy to consider.

Business/Non-Instructional Operations

Free or Reduced Price Lunches

Participation in the National School Lunch Program

Participation in the National School Lunch Program (NSLP) (and School Breakfast Programs) (SBP) is/are herewith authorized. Authorization is granted to the Superintendent to act on behalf of the Board for purposes of participating in the National School Lunch Program (and School Breakfast Program).

Free nutritious meals will be served to children from families whose income falls within the current criteria established by the Secretary of Agriculture under the Federal Lunch Program for free lunches.

The District shall establish an appeals process under which a parent/guardian may appeal a decision regarding his/her initial application for benefits, or any subsequent reduction or termination of benefits.

The schools shall not physically segregate or discriminate against any child because of his or her inability to pay for a meal. The names of children eligible to receive free meals shall not be published, posted, or announced in any manner; and there shall be no overt identification of any such children by use of special tokens or tickets, or by any other means.

The District shall ensure that, in the operation of the free and reduced-price meals and/or free milk programs, no student shall be discriminated against because of race, color, age, creed, religion, sex, sexual orientation, ancestry, gender identity or expression, national origin, marital status, pregnancy or disability, or any other basis prohibited by law, in its implementation of such a program.

The District's NSLP and SBP shall operate to meet dietary specifications in accordance with the Healthy, Hunger-Free Kids Act of 2010 and applicable state laws and regulations.

Note: *An optional approach, the Community Eligibility Provision (CEP) allows eligible schools to provide free meals to all students at no charge, regardless of family income. To qualify, at least 40 percent of a school's population must be identified as low income children who meet criteria for free school meals. Instead of collecting individual applications for free and reduced price meals, CEP uses information from other programs, including the Supplemental Nutrition Assistance Program and the Temporary Assistance Program for Needy Families.*

(cf. 3542 – School Lunch Program)
(cf. 3542.33 – Food Sales Other Than National School Lunch Program)
(cf. 3542.34 – Nutrition Program)
(cf. 3542.43 – Charging Policy)
(cf. 6142.101 – Student Nutrition and Physical Wellness, School Wellness)

Business/Non-Instructional Operations

Free or Reduced Price Lunches

Participation in the National School Lunch Program

Legal Reference: Connecticut General Statutes

10-215 Lunches, breakfasts and other feeding programs for public school children and employees. (as amended by PA 21-46)

10-216 Payment of expenses.

10-221o Lunch periods. Recess. Boards to adopt policies addressing limitations of physical exercise.

Title VII, Civil Rights Act, 42 U.S.C. 2000e, et seq. as amended by Title IX, Equal Employment Opportunity Act.

United States Department of Agriculture 7 C.F.R. 15, re nondiscrimination.

42 U.S.C. Sec. 1758, 7 CFR Part 145, Sec. 245.5, 245.6, 245.7, 210.9, 210.20

U.S.D.A., Eligibility Guidance for School Meals Manual

U.S.D.A., FNS Instruction 765-7 Rev. 2: Handling Lost, Stolen and Misused Meal Tickets

Healthy, Hunger-Free Kids Act of 2010, 42 U.S.C. 1751 §§203, 205

Nondiscrimination on the Basis of Handicap in Programs or Activities Receiving Federal Assistance, 7 C.F.R. Part 15b (2001)

Policy adopted:
rev 11/12
rev 1/15
rev 12/21

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

P.A. 18-125 AN ACT CONCERNING REVISIONS TO THE STUDENT DATA PRIVACY ACT

(Background Information for Policy Review Committee)

This Act makes numerous changes in the student data privacy law. The law restricts how website, online service, and mobile application (i.e., "online service") operators and consultants who contract with boards of education process and access student data. The law requires operators and consultants to use reasonable security practices to safeguard student data.

The Act requires the Commission for Educational Technology (CET) to develop a student data privacy terms-of-service agreement addendum that may be used in contracts entered into pursuant to the student data privacy law.

With respect to the privacy law, the legislation:

1. creates certain exceptions for contractors and operators from requirements for deleting student data at a board of education's, student's, parents', or guardians' request;
2. creates an exception, under certain conditions, for boards when they have special education students using a particular online service that is necessary, but unable to meet the contract requirements;
3. eliminates a requirement that boards electronically notify students and parents of new contracts;
4. requires the State Department of Education (SDE) to add more information to the guidance it must already provide school districts;
5. requires boards of education to annually report to CET on using any online service that does not operate under a contract as required by the law and the Act; and
6. adds the Connecticut Association of Schools' executive director, or his/her designee, as a member of the student data privacy task force.

The effective date of this legislation is July 1, 2018, except the provisions regarding the agreement addendum and the task force member are effective upon passage.

The new legislation does not change the definitions of contractor, operator or consultant, as used in the current policy sample.

The specific revisions contained in this legislation follow.

Sections 1 & 2 – Terms-of-Service Agreement Addendum

CET is required to develop a uniform student data privacy terms-of-service agreement addendum that may be used in contracts entered into pursuant to the privacy law. The addendum must conform to the requirements for a contract described in the law. CET must make the addendum available on its website or in an online registry it maintains for boards, contractors, and operators. It also authorizes boards of education and a contractor to include the addendum in any contract executed under this law to satisfy the law's requirements.

Section 2 – Special Education Student Exception

The Act exempts, under certain circumstances, a board of education from the requirement to enter into a contract that conforms with the privacy law's standards for students (1) receiving special education services or (2) who have an accommodation under the Rehabilitation Act of 1973 (commonly referred to as a Section 504 accommodation).

Under this legislation, this exemption only applies if the:

1. online service (a) is unique and necessary to implement the student's individualized education program (IEP) or Section 504 plan, (b) is unable to meet the law's contract requirements, and (c) complies with the federal Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA);
2. board can provide evidence it has made a reasonable effort to (a) enter into a contract with the online service and (b) find an equivalent online service that complies with the law; and
3. parent or legal guardian of the student, and, in the case of a student with an IEP, a member of the IEP planning and placement team, sign an agreement that (a) acknowledges that they are aware that the online service is unable to comply with the law and (b) authorizes the use of the service.

If such an exception is made, the online service must still comply with the security measures in the law, such as the data security and information deletion provisions and the general prohibition on disclosing, selling, or trading student information.

Under the Act, if a parent or legal guardian of a student requests the evidence of reasonable attempts to get the online service to agree to a contract or to find an equivalent service, the board must provide it.

Sections 2 & 3 – Deleting Student Data

Current law requires an operator or contractor to delete student records, student information, and student-generated content ("student information") in certain situations. It requires an operator to delete any student information, within a reasonable amount of time if a student, parent, legal guardian of a student, or board of education who has the right to control the student information requests its deletion.

This legislation creates an exception to this requirement when (1) state or federal law prohibits the deletion or requires retention of the information or (2) a copy of the student information is part of a disaster recovery storage system and is generally inaccessible to the public and the operator, provided a student, parent, or legal guardian or board of education may request it to be deleted if the operator uses it to repopulate accessible data after a disaster recovery.p

The Act also adds this exception to the provisions on student information deletion that must be in any contract between a board of education and a contractor.

Section 2 – Posting Contract Information

Current law 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 may be collected under the contract. The legislation removes the requirement to electronically notify students and parents. The law, unchanged by this Act, requires Boards remain required to post the notice and contract on their websites. This legislation requires boards each year by September 1, to electronically notify parents, guardians, and students of the website's address.

Section 2 – Exception for Retaining Information

Current law requires contracts for online services to include a statement that student information will not be kept by, or available to, the contractor after the contracted services are completed unless a student, parent, or guardian chooses to establish or maintain an account with the contractor. The Act specifies that the information will not be retained after the contract expires, rather than after the services are completed, and that the choice to establish or maintain an account takes place after the contract expires.

Section 4 – Guidance for School Districts

Existing law requires CET to provide guidance to boards on FERPA and the state privacy law. The bill requires SDE to add information on the terms-of-service agreement addendum to this guidance. It also requires SDE to consult with CET in providing the written guidance, which must include:

1. a plain language explanation of how FERPA and the state student data privacy law are to be implemented,
2. information about the terms-of-service agreement addendum, and
3. how the addendum can be incorporated into contracts executed under the state privacy law.

Section 5 – Student Data Privacy Task Force

By law, there is a task force to study student data privacy issues. The Act adds the Connecticut Association of Schools' executive director, or designee, as a member.

Section 6 – Reporting Requirement

The Act requires, every year beginning with the school year starting July 1, 2018, each board of education to submit a report to CET concerning the use of online services that do not have a contract that meets the standards required under the law and the Act. The report must indicate whether or not any of these online services are being so used, and, if so, a list of them.

The policy has been revised to reflect this legislation and follows.

July 2018

A policy to consider.

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 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 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 of Education 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 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.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

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

6. A description of the procedures that a contractor will follow for notifying the Board, in compliance with C.G.S. 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 of Education 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. (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.

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 the terms-of-service agreement addendum entered into between a contractor and the Board on or after July 1, 2018, 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 or the terms-of-service agreement addendum to include the missing provisions.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

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

Any contract entered into on and after July 1, 2018, or the terms-of-service agreement addendum 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 or the terms-of-service agreement addendum to include the required provisions.

The Board of Education shall maintain and update, as necessary, a website with information relating to all contracts entered into pursuant to this policy. Not later than five business days after executing a contract pursuant to this policy the Board shall post notice of such contract on the Board'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 Board of Education shall electronically notify students and the parents/guardians of students of the address of the Internet website described in this policy.

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

The Board of Education 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 Family Educational Rights and Privacy Act of 1974, 20 USC 1232g, as amended from time to time, and the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as amended from time to time, (2) the Board of Education 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 Board of Education shall, upon the request of a child's parent/legal guardian, provide the evidence described above to such parent/legal guardian.

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 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 Board 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 (3) how such addendum may be incorporated into contracts executed pursuant to section 10-234bb, as amended.

Notice of Breach of Security/Data Breaches

Upon notice of a breach of security by a contractor, the Board shall, not later than two business days after receipt of such notice, 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.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues

Notice of Breach of Security/Data Breaches (continued)

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.

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.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues

Definitions (continued)

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.
    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.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-Based Issues

Definitions (continued)

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.

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;
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.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

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

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 (app), 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;
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;
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.

Business and Non-Instructional Operations

Data-Based Information and Management Systems

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

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.

10-234aa Definitions

10-234bb Contracts between boards of education and contractors re student data. Requirements. (as amended by PA 18-125)

10-234cc Requirements for operators re student data

10-234dd Duties re unauthorized release, disclosure or acquisition of student data (as amended by PA 18-125)

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. 16-189 An Act Concerning Student Privacy

PA 17-200 An Act Making Revisions to the Student Data Privacy Act of 2016

PA 18-125 An Act Concerning Revisions to the Student Data Privacy Act

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).

Business and Non-Instructional Operations

Data-Based Information and Management Systems

Student Data Protection and Privacy/Cloud-based Issues

Legal Reference: (continued)

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
rev 7/17
rev 6/18

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

_____ 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: _____

A recommended policy to consider.

Business/Non-Instructional Operations

Hazardous Materials Communication

The Board of Education recognizes the necessity of utilizing hazardous materials in the day-to-day operation of school facilities and in supporting education requirements. The Board realizes that with the use of hazardous materials, responsibility must be taken to ensure personal safety and to protect the environment during use, storage and transportation. There are many areas of the District, from science laboratories and art departments to custodial services and vehicle maintenance, where such a variety of uses is performed.

Hazardous materials include any substance or mixture of substances that poses a fire, explosive, reactive or health hazard. Examples of materials classed as hazardous are: common household cleaning supplies, spray oven cleaners, cleaning solvents, photo chemicals, soldering flux, some ceramic glazes, oils and gasoline.

The Board, through the Superintendent, shall cause to be created, procedures which address the purchase, storage, handling, transportation and disposal of hazardous materials for school facilities and operations including instructional areas.

The goal of the procedures shall be to have in place an ongoing process by which each location in the District will have a program of identifying and managing hazardous materials. The Hazard Communication Program materials will be located in the school office. District personnel shall be encouraged to substitute non-hazardous materials for hazardous substances to the extent possible and to minimize the quantities of hazardous substances stored on school property.

Policy adopted:

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

POLICY SERVICES

An optional policy to consider.

Business/Non-Instructional Operations

Board of Education Credit Card

A credit card will be issued only in the name of the Board of Education. The credit card will be under the sole supervision of the Superintendent or the Business Manager, and only expenditures by Board employees to conduct business associated with the school system will be authorized by the Business Manager. The Board of Education credit card shall be used for school business only, not for any personal business. If the Board of Education credit card is used for personal business disciplinary action, which may include termination, will be taken.

Immediately subsequent to the use of the credit card, the Board employee will return the credit card and submit a fully itemized statement of expenses. The Board employee will pay any charges against the credit card not authorized, not properly identified on the statement of expenses, or disallowed following an internal or external audit.

An employee will not use the credit card if any of his/her disallowed charges are outstanding. The Board, Superintendent, or Business Manager has the unlimited authority to terminate the use of the credit card by any employee if there is any suspicion the use of the credit card is being abused in any manner.

Legal Reference: Connecticut General Statutes

10-248 Payment of school expenses.

Policy adopted:
cps 12/03

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

CURRENT POLICY

9130

Bylaws of the Board

Committees

Committees of the Griswold Board of Education shall be established, not later than one month after the date on which the newly elected BOE members take office, or as needed, by a majority vote of the Board.

Duties of each committee shall be determined as a committee is formed.

Each committee may make a report through its Chairperson at each regular meeting of the Board of Education.

No committee shall have power other than to recommend to the Board of Education unless specially authorized. No committee, or member of a committee, is authorized to make any contract or enter into any agreement which involves the expenditure of money, unless such contract or agreement is authorized by the Board either in regular or special meeting.

All committees of the Board of Education shall follow the provisions of the Freedom of Information Act as required by statute.

Special Committees/Temporary Committees/Ad Hoc Committees

In addition to the Standing Committees, the Chairperson of the Board of Education shall appoint temporary and special committees as may be deemed necessary or advisable by the Board of Education, and the Chairperson shall be an ex-officio member of each committee.

The duties of the committee shall be outlined at the time of appointment, and the committee shall be considered dissolved when its final report has been made to the Board of Education.

Record Keeping

All committees shall keep minutes of business conducted at meetings. The minutes will be kept on file in the Superintendent's office and available at all times to the Board of Education members. The minutes shall include the names of the committee members in attendance, listing of topics discussed and committee recommendations.

(cf. 9132 - Standing Committees)

(cf. 9133 - Special/Advisory Committees)

Legal Reference: Connecticut General Statutes

1-200 through 1-241 Freedom of Information Act.

1-200 Definitions.

1-225 Meetings of government agencies to be public.

Bylaw adopted by the Board: May 28, 2013

Bylaw revised by the Board: June 10, 2019

GRISWOLD PUBLIC SCHOOLS

Griswold, Connecticut

OTHER SAMPLES

Bylaws of the Board

Committees

In order to expedite smooth functioning, the Board authorizes the establishment of such standing and/or temporary committees as it finds necessary to study operations in specific areas and to make recommendations for Board policy and action.

The following procedures will govern the appointment and function of such committees:

1. Standing committees and their chairpersons shall be appointed biennially by the Board Chairperson at the first regular meeting following the organizational meeting. The Board has authorized the following standing committees: curriculum, finance, personnel, planning, public information, policy, transportation, liaison, legislative;
2. The Board Chairperson shall be an ex officio member of all standing committees;
3. The Chairperson of the Board of Education shall appoint temporary and special committees as may be deemed necessary or advisable by the Board of Education, and the Chairperson shall be an ex officio member of each committee; and
4. The duties of the committee shall be outlined at the time of appointment, and the committee shall be considered dissolved when its final report has been made to the Board of Education.

No committee shall have power other than to recommend to the Board of Education unless specially authorized. No committee, or member of a committee, is authorized to make any contract or enter into any agreement which involves the expenditure of money, unless such contract or agreement is authorized by the Board whether in regular or special meeting.

All committees of the Board of Education shall follow the provisions of the Freedom of Information Act as required by statute.

All committees shall keep minutes of business conducted at meetings. The minutes will be kept on file in the Superintendent's office and available at all times to Board of Education members.

Legal Reference: Connecticut General Statutes
1-200 through 1-241 Freedom of Information Act
1-200 Definitions
1-225 Meetings of government agencies to be public

Bylaw adopted by the Board:

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

Sample bylaw.

Bylaws of the Board

Committees

Committees of the _____ Board of Education shall be established at the first regularly scheduled meeting in December, or as needed, by a majority vote of the Board.

Duties of each committee shall be determined as a committee is formed.

Each committee may make a report through its Chairperson at each regular meeting of the Board of Education. Each committee shall make its annual report at the meeting **prior to** the first regularly scheduled meeting in December.

No committee shall have power other than to recommend to the Board of Education unless specially authorized. No committee, or member of a committee, is authorized to make any contract or enter into any agreement which involves the expenditure of money, unless such contract or agreement is authorized by the Board either in regular or special meeting.

All committees of the Board of Education shall follow the provisions of the Freedom of Information Act as required by statute.

The Board of Education shall act as a committee of the whole in final consideration of all matters.

Record Keeping

All committees shall keep minutes of business conducted at meetings. The minutes will be kept on file in the Superintendent's office and available at all times to the Board of Education members. The minutes shall include the names of the committee members in attendance, listing of topics discussed and committee recommendations.

(cf. 9131 – Committee of the Whole)
(cf. 9132 - Standing Committees)
(cf. 9133 - Special/Advisory Committees)

Legal Reference: Connecticut General Statutes
1-200 through 1-241 of the Freedom of Information Act.
1-200 Definitions.
1-225 Meetings of government agencies to be public.

Bylaw adopted by the Board:
cps 4/99
rev. 1/06

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

OTHER SAMPLES

Bylaws of the Board

Committees

In order to expedite smooth functioning, the Board authorizes the establishment of such standing and/or temporary committees as it finds necessary to study operations in specific areas and to make recommendations for Board policy and action.

The following procedures will govern the appointment and function of such committees:

1. Standing committees and their chairpersons shall be appointed biennially by the Board Chairperson at the first regular meeting following the organizational meeting. The Board has authorized the following standing committees: curriculum, finance, personnel, planning, public information, policy, transportation, liaison, legislative;
2. The Board Chairperson shall be an ex officio member of all standing committees;
3. The Chairperson of the Board of Education shall appoint temporary and special committees as may be deemed necessary or advisable by the Board of Education, and the Chairperson shall be an ex officio member of each committee; and
4. The duties of the committee shall be outlined at the time of appointment, and the committee shall be considered dissolved when its final report has been made to the Board of Education.

No committee shall have power other than to recommend to the Board of Education unless specially authorized. No committee, or member of a committee, is authorized to make any contract or enter into any agreement which involves the expenditure of money, unless such contract or agreement is authorized by the Board whether in regular or special meeting.

All committees of the Board of Education shall follow the provisions of the Freedom of Information Act as required by statute.

All committees shall keep minutes of business conducted at meetings. The minutes will be kept on file in the Superintendent's office and available at all times to Board of Education members.

Legal Reference: Connecticut General Statutes
1-200 through 1-241 Freedom of Information Act
1-200 Definitions
1-225 Meetings of government agencies to be public

Bylaw adopted by the Board:

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

Sample bylaw.

Bylaws of the Board

Committees

Committees of the _____ Board of Education shall be established at the first regularly scheduled meeting in December, or as needed, by a majority vote of the Board.

Duties of each committee shall be determined as a committee is formed.

Each committee may make a report through its Chairperson at each regular meeting of the Board of Education. Each committee shall make its annual report at the meeting **prior to** the first regularly scheduled meeting in December.

No committee shall have power other than to recommend to the Board of Education unless specially authorized. No committee, or member of a committee, is authorized to make any contract or enter into any agreement which involves the expenditure of money, unless such contract or agreement is authorized by the Board either in regular or special meeting.

All committees of the Board of Education shall follow the provisions of the Freedom of Information Act as required by statute.

The Board of Education shall act as a committee of the whole in final consideration of all matters.

Record Keeping

All committees shall keep minutes of business conducted at meetings. The minutes will be kept on file in the Superintendent's office and available at all times to the Board of Education members. The minutes shall include the names of the committee members in attendance, listing of topics discussed and committee recommendations.

(cf. 9131 – Committee of the Whole)
(cf. 9132 - Standing Committees)
(cf. 9133 - Special/Advisory Committees)

Legal Reference: Connecticut General Statutes
1-200 through 1-241 of the Freedom of Information Act.
1-200 Definitions.
1-225 Meetings of government agencies to be public.

Bylaw adopted by the Board:
cps 4/99
rev. 1/06

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

CURRENT POLICY

Bylaws of the Board

Formulation, Adoption, Amendment of Policies

The Griswold Board of Education considers policy development its chief function, along with appraisal of the result achieved through its policies. It is through the development and adoption of written policies that the Board shall exercise its leadership in the operation of the school system; it is through study and evaluation of reports concerning the execution of its written policies that the Board shall exercise its control over school operations.

Within the context of current law, the District shall be guided by Board-adopted written policies that are given appropriate distribution and are accessible to staff members, parents, students, and community residents.

Local policies become effective upon Board adoption or at a future date designated by the Board at the time of adoption.

Written policies serve as guides for the discretionary action of those to whom it delegates authority and as a source of information and guidance for all persons who are interested in, and affected by, the district schools.

Changes in needs, conditions, purposes, and objectives will require revisions, deletions, and additions to the policies of present and future Boards. Thus policy development is an ongoing process.

Policy Draft Writer

The Superintendent or designee shall be responsible for recasting Board consensus about policy recommendations into acceptable written form for further deliberation and/or action by the Board.

Attorney Involvement In Policy Development

The Superintendent, as the policy draft writer for the Board, shall seek the advice of counsel when, in the Superintendent's opinion or the Board's, there may be a question of legality or proper legal procedure in the development of a proposed policy.

In the development of policies, the Board will delegate the Superintendent the responsibility of seeking the advice and counsel of appropriate personnel.

The purpose of this provision is that the Board may gain the most complete and reliable information possible on which to base decisions.

Policy Adoption

Adoption of new policies or changing existing policies is solely the responsibility of the Board.

Policies will, barring extenuating circumstances, be adopted or amended after consideration at two meetings of the Board of Education. The time between Board meetings shall permit further study and also give an opportunity to interested parties to react; however, approval may be granted by the Board to meet extenuating circumstances or special events.

The agenda and minutes shall be marked to indicate policy matters. The formal adoption of policies shall be by majority vote of present members of the Board of Education and the action shall be recorded in the minutes of the Board of Education. Only those written statements so adopted and so recorded shall be regarded as official policy.

Policy Dissemination

The Superintendent is directed to establish and maintain an orderly plan for making pertinent policies of the Board known to staff members, students, and others affected by them.

The Superintendent shall arrange to disseminate to staff members all new policies that affect them and their work and shall also provide easy accessibility to an up-to-date policy collection for all employees of the school system and members of the Board.

The Board's policy manual shall be considered a public record and shall be open for inspection at the Board offices. The Board's policy manual is available on the district web site, and upon request, printed copies are available at the district's central office.

Reference: Robert's Rules of Order, Revised

Bylaw adopted by the Board: May 28, 2013

Bylaw revised by the Board: June 10, 2019

GRISWOLD PUBLIC SCHOOLS

Griswold, Connecticut

OTHER SAMPLES

Bylaws of the Board

Formulation, Adoption, Amendment of Policies

Policy proposals and suggested amendments to, deletions of, or revisions of existing policies shall normally be submitted to all members of the Board of Education by the Superintendent in writing prior to a regularly scheduled Board of Education meeting in which such proposed policies, amendments or revisions thereof shall be read and discussed. Policies that deal with matters of an emergency may be introduced at any regular or special Board meeting.

Policies will, unless by vote of two-thirds of the members present of the Board of Education, be adopted or amended after consideration at two regular meetings of the Board of Education. The agenda and minutes shall be marked to indicate policy matters.

The formal adoption of policies shall be by two-thirds vote of all members present of the Board of Education and the action shall be recorded in the minutes of the Board of Education. Only those written statements so adopted and so recorded shall be regarded as official policy.

Alternate Language: The format adoption or deletion of policies and the adoption of policy changes shall be by majority vote of all members of the Board, and the action shall be recorded in the minutes of the Board of Education.

Additional Language to Consider: Policies that affect students shall become effective at the beginning of the next school year following adoption unless the policy provides otherwise.

Reference: Robert's Rules of Order, Newly Revised

Bylaw adopted by the Board:

rev 11/20

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

Sample bylaw to consider.

Bylaws of the Board

Formulation, Adoption, Amendment of Policies

The _____ Board of Education considers policy development its chief function, along with appraisal of the result achieved through its policies. It is through the development and adoption of written policies that the Board shall exercise its leadership in the operation of the school system; it is through study and evaluation of reports concerning the execution of its written policies that the Board shall exercise its control over school operations.

It is the intent of the Board to develop policies and put them in writing so that they serve as guidelines and goals for the successful and efficient functioning of the public schools.

Written policies serve as guides for the discretionary action of those to whom it delegates authority and as a source of information and guidance for all persons who are interested in, and affected by, the district schools.

Changes in needs, conditions, purposes, and objectives will require revisions, deletions, and additions to the policies of present and future Boards. Thus policy development is an ongoing process.

Policy Draft Writer

The Superintendent or designee shall be responsible for recasting Board consensus about policy recommendations into acceptable written form for further deliberation and/or action by the Board.

Attorney Involvement in Policy Development

The Superintendent, as the policy draft writer for the Board, shall seek the advice of counsel when, in the Superintendent's opinion or the Board's, there may be a question of legality or proper legal procedure in the development of a proposed policy.

In the development of policies, the Board will delegate the Superintendent the responsibility of seeking the advice and counsel of appropriate personnel.

The purpose of this provision is that the Board may gain the most complete and reliable information possible on which to base decisions.

Policy Adoption

Adoption of new policies or changing existing policies is solely the responsibility of the Board.

Bylaws of the Board

Formulation, Adoption, Amendment of Policies

Policy Adoption (continued)

Policies will, except for emergency situations, be adopted or amended after consideration at two meetings of the Board of Education. The time between Board meetings shall permit further study and also give an opportunity to interested parties to react, however, temporary approval may be granted by the Board in lieu of formal policy to meet emergency conditions or special events which will take place before formal action can be taken.

The agenda and minutes shall be marked to indicate policy matters. The formal adoption of policies shall be by majority vote of present members of the Board of Education and the action shall be recorded in the minutes of the Board of Education. Only those written statements so adopted and so recorded shall be regarded as official policy.

Policies that deal with matters of an emergency nature may be introduced at any regular or special Board meeting.

Policy Dissemination

The Superintendent is directed to establish and maintain an orderly plan for making pertinent policies of the Board known to staff members, students, and others affected by them.

The Superintendent shall arrange to disseminate to staff members all new policies that affect them and their work and shall also provide easy accessibility to an up-to-date policy collection for all employees of the school system and members of the Board.

The Board's policy manual shall be considered a public record and shall be open for inspection at the Board offices.

Reference: Robert's Rules of Order, Revised

Bylaw adopted by the Board:

rev 11/20

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.

Another version of this bylaw.

Bylaws of the Board

Policies

Introduction

Board of Education policies translate beliefs and desires of elected officials into action through the Superintendent of Schools and the school staff. Except for specific meeting decisions, policies are a Boards' best means of shaping district education through specifying in Board policy "what will be done." The Superintendent's administrative regulations provide the administrative "how it will be done" to accompany Board of Education policies

Policies also make it clear, at least by implication, that Superintendents are expected to follow the direction of the entire Board as it is expressed through its policies. On a daily basis, Board policies, except for bylaws, are primarily for the guidance of the Superintendent of Schools and his/her staff. It is, however, the Board's responsibility to ensure the Superintendent uses policies in making decisions; it is, similarly, the Superintendent's responsibility to insist that both policies and their amplifying regulations are followed by everyone in the school system.

Organization and Contents of Policy Manuals

Policy manuals contain three basic types of entries — Board of Education policies, Superintendent of Schools regulations, and Board of Education bylaws:

1. Policies are guides for discretionary action by the Superintendent of Schools and staff; not all policies require administrative regulations;

2. Regulations are the Superintendent's amplifications of Board policies into specific staff actions; not all administrative regulations require policies;

3. Bylaws are rules governing Boards of Education's internal operations.

Development of Board Policies

The development of sound educational policies is one of the primary duties of the Board of Education. Policies serve to promote democratic and responsive school governance and constitute a major method by which the Board exercises its leadership. Policies are guides for discretionary administrative action by the Superintendent of Schools and his/her staff. Policy development and revision should follow these principles:

1. Policies and regulations shall be given high priorities by the Board and by the Superintendent of Schools;

2. Many people at different levels shall be given opportunities to participate in development and review of policies and regulations;

Bylaws of the Board

Policies

Development of Board Policies (continued)

3. Procedures for development and revision of policies and regulations shall be clear and well understood; participants shall know their roles and authority; lines of communication shall be observed;

4. Use of policies and regulations as guides to action shall be stressed at all organizational levels, and policy or regulatory violations shall not be overlooked or condoned;

5. Policy and regulatory effectiveness shall be monitored regularly by the Board of Education, the Superintendent of Schools, and by other staff members;

6. Board members and administrators shall guard against intrinsic problems of policies and regulations. *(rigidity and inflexibility, bureaucratic or insensitive administration of policy, etc.)*

Anyone may propose a new policy or policy changes — members of the community, the staff, students, Superintendent, or Board members. Proposed new policies and policy changes from staff shall be forwarded to the Superintendent for presentation to the Board. Although the Board encourages and welcomes community, staff and student involvement, only the Board may establish policy.

The Superintendent is encouraged to submit written recommendations for new policies and for revision of existing policies as necessary for the effective operation of the public schools.

Approved policies shall be in writing and coded according to the policy codification system approved by the Board, and made part of the official policy manual maintained by the Superintendent. Policy manuals and copies of new and changed policies shall be distributed to all members of the Board of Education and school administrators, and shall be made available to the staff, students, and general public.

Adoption and/or Amendment of Board of Education Policies

Procedure for the adoption of a new policy or the amendment of existing policy shall be:

1. Upon referral to the policy committee, the committee will develop a statement of policy or change of existing policy based on the following:

    a. Suggestions and requests from Board members;

    b. Recommendations from the Superintendent of Schools;

Bylaws of the Board

Policies

Adoption and/or Amendment of Board of Education Policies (continued)

c. Statutory requirements;

d. Citizen input.

2. The policy committee shall present a policy statement, or revised policy statement, with its recommendations to the Board at a regular Board meeting. No action shall be taken at this presentation meeting.

3. The Board shall act on proposed policies at regular meetings of the Board at which time amendments to the policy proposals may be made and the policies approved if the changes are not a departure from the essence of the policy proposal; if the proposed changes are major, a policy should be brought back for a second review at the next regular meeting with a further recommendation from the Board's policy committee. Proposed policy changes approved by majority vote of the Board shall take immediate effect.

4. For proposed policy statements, new or revised, because of changes or additions to Connecticut General Statutes or State Board of Education Regulations, approval may be given at the initial presentation.

Formal adoption of policies and/or amendments of policies shall be recorded in the minutes of the Board meeting. Only those written statements so adopted and recorded shall be regarded as official policies.

Legal Reference: Connecticut General Statutes

10-221 Boards of education to prescribe rules, policies, and procedures.

Bylaw adopted by the Board:

Sample policies are distributed for demonstration purposes only. Unless so noted, contents do not necessarily reflect official policies of the Connecticut Association of Boards of Education, Inc.