Policies for Review – 2nd Reading

January 8, 2024

GBCD – Background Investigation and Criminal History Records Check

EHAB – Data Governance and Security

EBCC – False Alarms, Bomb, Active Shooter and Other Such Threats

FA – Facilities Development Goals and Preparation of Capital Improvement Plan

FAA – Annual Facility Plan and Unused District Property

BACKGROUND INVESTIGATION AND CRIMINAL HISTORY RECORDS CHECK

To help assure the safety of District students, it is the policy of the Gilford School Board that before any person is employed by the School District, or are otherwise placed into positions whereby they have frequent close contact with - or supervision of - students, that the administration conduct proper investigation into such person's background, including, without limitation, a criminal history records check under RSA 189:13-a – 189:13-c.

A. Definitions. As used in this policy:

1. **"Applicant"** shall mean and include an applicant for employment or any person seeking to serve in any position falling within the term "Covered Person" as defined below, who is selected by the District for further consideration for such position.
2. **"Background investigation"** means an investigation into the past employment and other background of an Applicant with the intent of determining whether:
    a. The applicant/covered person is qualified for the position for which the person has applied, will/would be assigned, or will/would perform, and
    b. The applicant has been found guilty of any criminal activity or conduct that would make the applicant ineligible or unsuitable for employment or service in the district.
3. **"Conditional offer of employment"** means an offer of employment extended to a selected Applicant subject to a successful completed criminal history record check (defined below) which is satisfactory to the SAU or school district.
4. **"Contractor"** means a private business or agency or an employee or employees of the contractor which contracts with a SAU or school district to provide services including but not limited to:
    a. cafeteria workers,
    b. school bus drivers,
    c. custodial personnel,
    d. any other direct service or services to students of the district.
5. **"Covered Person"** shall mean every employee, stipend position (e.g., coach, trainer, drama coach, etc.), candidate, designated volunteer (whether direct or through a volunteer organization), or any other service where the contractor or employees of the contractor provide services directly to students of the District or any applicant/person seeking to serve in any of those positions. NOTE: Only those volunteers who meet the definition of "Designated Volunteer" below are considered "Covered "Employees". See Board policy IJOC for additional provisions relating to all volunteers. All Covered Persons are required to undergo training as provided in Board policy GBCE.
6. **"Criminal History Records Check" or "CHRC"** means a criminal history records inquiry under RSA 189:13-a – 13-c, conducted by the New Hampshire State Police through its records and through the Federal Bureau of Investigation.
7. **"Volunteer"** is defined as an individual that provides services whether for classroom or other student programs or activities, chaperones, classroom volunteers, trades work, etc.

8. **"Designated Volunteer"** is any volunteer who:
    a. Comes in direct contact with students on a predictable basis (e.g., library volunteer, overnight field trip chaperone;
    b. Meets regularly with students (e.g., community mentor, volunteer assistant coach);
    c. Meets with students on a one-on-one basis without the presence of a teacher or other such professional staff member; OR
    d. Any other volunteer so designated by the School Board or Superintendent.

    The administrative supervisor for the applicable activity or program (e.g., building principal, athletic director), shall have the responsibility of determining whether a volunteer position is a "Designated Volunteer", subject to any additional rules or procedures established by the Superintendent.
9. **"Educator Candidate"** means a student at an institution of higher education in New Hampshire who has been selected to participate in a K-12 educator preparation program (RSA 189:13-c, I(b)). This definition includes both Educator Candidates who are placed as student teachers in the district, and those who might be in the District for a different purpose (e.g., Methods, etc.).
10. **"Section V Offense(s)"** are those criminal offenses listed in RSA 189:13-a, V, as that list may be amended by the Legislature from time to time. The current of offenses may be accessed at:

    http://www.gencourt.state.nh.us/rsa/html/XV/189/189-13-a.htm

    "Non-Section V Offenses" are all other crimes offenses, whether felonies or misdemeanors.

11. **"Designee"** shall mean, a person designated by the Superintendent to receive and inspect results of the Criminal History Records Check. Under RSA 189:13-a, II, the designee for purposes of CHRC may only be the head of human resources, the personnel director, the business administrator or the finance director.

B. Background Investigation and Restrictions on Hiring or Appointing Individuals with Revoked or Suspended Credentials.

1. General Requirements. The Superintendent will require a Background Investigation of any Applicant or Covered Person as defined in this policy, *including but not limited to reviewing the most recent NHED List of Revoked & Suspended Credentials.* The Superintendent may assign the Background Investigation (but not the CHRC) to someone other than Designee, but the Background Investigation shall be completed prior to making a final offer of employment, approving the contract with an individual contracting directly with the District, student teacher, or a Designated Volunteer to work or serve within the District. For Covered Persons who are employed by a third-party contractor or assigned as a Designated Volunteer by a volunteer agency, the Superintendent or Designee may waive the Background Investigation and instead rely on

suitable assurances from the contracting company or agency regarding a background investigation. The requirement for a Criminal History Records Check under paragraph D, below, however, may not be waived. *All decisions regarding employment and the pre-employment process shall conform to the District's Anti-Discrimination and Equal Opportunity policy, AC.*

As part of the application process, each Applicant shall be asked if they have ever been convicted of any crime and whether there are any criminal charges pending against the applicant at the time of application. The Applicant will also be directed to report any criminal charges brought against them after the application is submitted and until either hired or until notified that they will not be hired. Failure to report will be treated in the same manner as falsification of information under Section C, below.

General record (e.g., checklist and or source documentation) of completion of a Background Investigation (but not copies of the results of a CHRC) shall be retained in an employee's personnel file and retained pursuant to the District's Record Retention Schedule EHB-R.

2. Prohibition against hiring/appointment of individuals with revoked or suspended credentials. The District will not hire any individual whose education license, certification or other credential ("credential") issued by the Department of Education is currently revoked or suspended, unless: (1) the individual's prospective employment would begin after the reinstatement of that individual's credential; or, (2) the individual retains an active endorsement in one or more areas in which the individual remains eligible for employment, even though the endorsement in another area is under revocation or suspension.

   No person whose credential issued by the Department of Education has been revoked or is under current suspension, may be appointed as, or serve as, a volunteer for any district service or activity, designated or otherwise.

   In the instance of a person with no current endorsement, the suspension or revocation would preclude hiring or appointing that person to any position within the district. This means, for example, that a former science teacher whose credentials are revoked may not be appointed as a volunteer soccer coach.

   Notwithstanding the prohibitions and limitations imposed by this paragraph, educators whose credentials have been revoked or are currently suspended, retain all the rights afforded members of the public to enter onto school grounds and attend school events in accordance with applicable laws and School Board policies. Similarly, such individuals who are parents or guardians of district students shall maintain all the rights afforded all

parents and guardians under law and School Board policies – but may not serve in volunteer positions.

B. False Information. The falsification or omission of any information on a job application, during the pendency of the 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, withdrawal of any offer of employment, or immediate discharge from employment.

C. Criminal History Records Check.

1. **General.** As part of the District's Background Investigation, each Applicant must submit to a Criminal History Records Check ("CHRC") through the State of New Hampshire in full compliance with RSA 189:13-a. No Covered Person/Applicant shall be employed, extended a Conditional Offer of Employment, or begin service in the District, until the Superintendent, or designee, has initiated a CHRC.

   The Applicant shall provide the District with a criminal history records release form as provided by the New Hampshire State Police along with a full set of fingerprints taken by a qualified law enforcement agency according to RSA 189:13-a, II.

   Refusal to provide the required criminal history records release form (with fingerprints) and any other required releases to authorize the CHRC will result in immediate disqualification of the Applicant/Covered Person and will not be considered for the position.

2. **Special Provisions for Educator Candidates, Bus Drivers**

   a. **Educator Candidate.** Educator Candidates who are placed in the District as a student teacher shall undergo a CHRC prior to beginning in the District. For Educator Candidates in the District under a status other than student teacher (e.g, observation, Methods Course or Practicum student), the Superintendent or designee will determine whether to require a CHRC using the same parameters included in the Designated Volunteer definition, above.
   b. **Bus Drivers.** Pursuant to RSA 189:13-a, VI and RSA 189:13-b, criminal history records checks for bus drivers shall be processed through the New Hampshire Department of Education ("NHED"). Although NHED will conduct the CHRC, the Superintendent or designee shall require a Background Investigation in accordance with paragraph B.

3. **Results of Criminal History Records Check.** The results of the CHRC shall be delivered to the Superintendent or designee who shall be responsible for maintaining their confidentiality. The Superintendent or designee shall destroy all results and reports of any CHRC within sixty (60) days of receiving said information.

4. **Pending Charges or Convictions for Section V Offenses.** If the results of the CHRC disclose that the Applicant has either been convicted of or is charged pending disposition of a violation or attempted violation of a Section V offense, that person shall not receive an offer or final offer of employment. Additionally, the Superintendent (not the Superintendent's designee), shall notify NHED through its Investigator or the Chief of the Governance Unit or as otherwise directed by NHED.

5. **Non-Section V Offenses and/or Past Charges of Section V Offenses.** If the results of a CHRC disclose that the Applicant has been charged (whether pending or previously concluded) with a Non-Section V Offense, or has been previously charged with a Section V Offense which the charge has been disposed of other than by a conviction, the Superintendent or designee shall take such information into account prior to hiring or assigning such Applicant. In making a determination regarding such an Applicant, the Superintendent or designee shall consider all reliable information, and assess whether, in light of the totality of the circumstances, the Applicant's suitability for the position sought with student safety being the priority consideration. (Circumstances the Superintendent should consider, include, but are not limited to, nature and date of the charge, information about reduced charges, age at time of charge, relationship of the nature of the charged offense to the duties of the position sought).

   If the Superintendent chooses to nominate, appoint or assign an Applicant who has a history of conviction or pending charges of a Non-Section V Offense, or of past concluded charges of Section V Offenses that did not result in a conviction, then the final hiring decision or appointment of another Covered Person must be approved by the School Board. Pursuant to regulations of the United States Dept. of Justice, and RSA 189:13-a, the Superintendent may not share with the Board information directly gleaned from the CHRC regarding specific criminal charges, arrests, convictions etc., but may share the fact that s/he is nominating a person whose background investigation revealed information requiring the Superintendent to apply the criteria established by the Board in the preceding paragraph.

6. **Fees for Criminal History Records Check.** Any applicant for whom the Board requires a CHRC check, or, in the instance of third party contractors/organizations, the Covered Person's employer/organization, shall pay the actual fees and costs associated with the fingerprinting process and/or the submission or processing of the CHRC, unless otherwise determined by the Board.

7. **Additional Criminal Records Checks.** To the extent permitted by law, the Superintendent or designee may require a CHRC of any Covered Person at any time after hire or appointment to a position within the District.

D. Conditional Offer of Employment. Applicants who have been selected for employment may be given a conditional offer of employment, with the final offer subject to the successful completion

of the Background Investigation and CHRC, and a determination that there are no disqualifying pending charges or convictions. Any Applicant who is offered conditional employment, by way of individual contract or other type of letter of employment, will have clearly stated in such contract or letter of employment that employment or approval to work within the District is entirely conditioned upon the results of a CHRC and Background Investigation being satisfactory to the District.

E. Final Offer of Employment. No Applicant shall be extended a final offer of employment or be allowed to serve/provide services in the District if such person has charges pending or has been convicted of any Section V Offense; or where such person has been convicted of the same conduct in another state, territory, or possession of the United States; or where such person has been convicted of the same conduct in a foreign country.

An Applicant may only be extended a final offer of employment or final approval to work/serve within the District's schools upon the satisfactory completion and results of CHRC and Background Investigation.

F. Administrative Protocols/Procedures. The Superintendent is authorized to establish written protocols for background investigations, and such protocols may vary depending on the nature of the position(s) (e.g., verification of academic records and achievements for certified professionals, credit checks for personnel with fiscal responsibilities). The written protocols may include additional specific disqualifying misdemeanor or felony convictions or charges (e.g., prostitution, theft, etc.) in addition to the Section V Offenses.

G. Contractor and Vendor Provisions. The Superintendent shall take such steps as are necessary to assure third party agreements which involve covered personnel to include a provision for such personnel to complete CHRCs and Background Investigations as required under this policy, as well as training and information relative to child sexual abuse prevention as required under RSA 189:13-a, XII and policy GBCE.

H. Training of Superintendent/Designee. The Superintendent or any designee shall complete such training relative to the reading and interpretation of criminal records as required by NHED.

I. Reports of Criminal Offenses Post-Hire or Commencement of Service. When the District receives a notification of a Covered Person being charged with or convicted of a Section V Offense or other crime which is evidence of the individual's unsuitability to continue in their role, the Superintendent shall take immediate appropriate action to remove the individual from contact with students. Employees shall be placed on paid administrative leave, if not subject to immediate discharge. The Superintendent will then take appropriate employment or other action, consistent with law and any applicable employment contract or collective bargaining agreement to address the individual's ongoing relationship with the District. If the Covered Person charged/convicted of a Section V Offense is a credential holder as defined in the New Hampshire Code of Conduct for Educators, the Superintendent shall report to the New Hampshire

Department of Education pursuant to section 510.05 of the Code and Board policy GBEAB – Mandatory Code of Conduct Reporting.

Legal References:

RSA 189:13-a, School Employee and Designated School Volunteer Criminal History Records Check
RSA 189:13-b, School Bus Driver and Transportation Monitor Criminal History Records Check
Code of Conduct for New Hampshire Educators
RSA 189:13-c Credentialing Applicant and Candidate Criminal History Records Check

Current GSD policy. Policy Committee suggests updating with NHSBA sample policy due to passage of SB213.
11-17-2023 Policy Committee
12-4-2024 First Reading
12-8-2023 Sent to GEA
1-8-2024 Second Reading

DATA GOVERNANCE AND SECURITY

To accomplish the District's mission and comply with the law, the District must collect, create and store information. Accurately maintaining and protecting this data is important for efficient District operations, compliance with laws mandating confidentiality, and maintaining the trust of the District's stakeholders. All persons who have access to District data are required to follow state and federal law, District policies and procedures, and other rules created to protect the information.

The provisions of this policy shall supersede and take precedence over any contrary provisions of any other policy adopted prior to the date of this policy.

A. Definitions

Confidential Data/Information - Information that the District is prohibited by law, policy, or contract from disclosing or that the District may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information regarding students and employees.

Critical Data/Information - Information that is determined to be essential to District operations and that must be accurately and securely maintained to avoid disruption to District operations. Critical data is not necessarily confidential.

Cybersecurity Incident – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information processes, stores, or transmits, if that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

B. Data and Privacy Governance Plan - Administrative Procedures.

1. Data Governance Plan. The Superintendent, in consultation with the District Information Security Officer ("ISO") (see paragraph C, below), shall update the Data and Privacy Governance Plan ("Data Governance Plan") for presentation to the Board no later than June 30 each year.

   The Data Governance Plan shall include:

   (a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use;

   (b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed minimum standards set by the New Hampshire Department of Education;

   (c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools, and extensions used on District hardware, server(s) or through the District network(s);

   (d) A response plan for any breach of information/cybersecurity incidents; see RSA 31:103-b and RSA 359-C:19-21; and

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

The Data Governance Plan shall include standards and provisions that meet or exceed the standards set forth in the N.H. Dept. of Education's *Minimum Standards for Privacy and Security of Student and Employee Data.*

2. Policies and Administrative Procedures. The Superintendent, in consultation with the ISO, is directed to review, modify and recommend policies and administrative procedures where necessary. Such policies and/or procedures may or may not be included in the annual Data Governance Plan.

C. Information Security Officer.

The Director of Technology is hereby designated as the District's Information Security Officer (ISO) and reports directly to the Superintendent or designee. The ISO is responsible for implementing and enforcing the District's security policies and administrative procedures applicable to digital and other electronic data, and suggesting changes to these policies, the Data Governance Plan, and procedures to better protect the confidentiality and security of District data. The ISO will work with both the District and building level administrators and Data managers (paragraph E, below) to advocate for resources, including training, to best secure the District's data.

The IT Support Coordinator is the District's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

D. Responsibility and Data Stewardship.

All District employees, volunteers and agents are responsible for accurately collecting, maintaining, and securing District data including, but not limited to, confidential and/or critical data/information.

E. Data Managers.

All District administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the District's data inventory. Data managers will monitor employee access to the information to ensure that confidential information is accessed only by employees who need the information to provide services to the District and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISO in enforcing District policies and procedures regarding data management.

F. Confidential and Critical Information.

The District will collect, create or store confidential information only when the Superintendent or designee determines it is necessary, and in accordance with applicable law. The District will provide access to confidential information to appropriately trained District employees and volunteers only when the District determines that such access is necessary for the performance of their duties. The District will disclose confidential information only to authorized District contractors or agents who

need access to the information to provide services to the District and who agree not to disclose the information to any other party except as allowed by law and authorized by the District.

District employees, contractors and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise.

The Superintendent and/or the ISO shall immediately report any known or suspected cybersecurity incidents within the District's information systems, or within an information system of any vendor of the District, to the New Hampshire Cyber Integration Center of the Department of Information Technology. The Superintendent and/or the ISO shall disclose all known information and interactions. See RSA 31:103-b.

The ISO or designee will investigate immediately and take any action necessary to secure the information, issue all required legal notices and prevent future incidents. When necessary, the Superintendent, ISO, or designee is authorized to secure resources to assist the District in promptly and appropriately addressing a security breach.

As a part of this investigation, the ISO or designee will promptly determine the likelihood that any information part of a cybersecurity incident has been or will be misused. If the determination is that the misuse of information has occurred or is reasonably likely to occur, or if a determination cannot be made, the ISO will notify the affected individuals as soon as possible, consistent with the notification requirements under RSA 359-C:20.

Likewise, the District will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure.

All District staff, volunteers, contractors, and agents who are granted access to critical or confidential information/data are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of such confidential or critical data/information. All individuals using confidential and critical data/information will strictly observe all administrative procedures, policies, and other protections put into place by the District including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information no longer needed in a confidential and secure manner.

G. Using Online Services and Applications.

District staff members are encouraged to research and utilize online services or applications to engage students and further the District's education mission. District employees, however, are prohibited from installing or using applications, programs or other software, or online websites, that either stores, collects, or shares confidential or critical data/information, until the ISO approves the vendor and the software or service used. Before approving the use or purchase of any such software or online service, the ISO or designee shall verify that it meets the requirements of the law, Board policy and the Data Governance Plan.

H. Training.

The ISO will provide appropriate training to employees who have access to confidential or critical information to prevent unauthorized disclosures or breaches in security. All school employees will receive annual training in the confidentiality of student records, and the requirements of this policy and related procedures and rules.

I. Data Retention and Deletion.

The ISO or designee shall establish a retention schedule for the regular archiving and deletion of data stored on District technology resources. The retention schedule should comply with, and be incorporated into the data/record retention schedule established under Board policy EHB and administrative procedure EHB-R, including but not limited to, provisions relating to Litigation and Right to Know holds as described in Board policy EHB.

J. Consequences

Employees who fail to follow the law, or District policies or procedures, regarding data governance and security (including failing to report) may be disciplined, up to and including termination. Volunteers may be excluded from providing services to the District. The District will end business relationships with any contractor who fails to follow the law, District policies or procedures, or the confidentiality provisions of any contract. In addition, the District reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

The District may suspend all access to data or use of District technology resources pending an investigation. Violations may result in temporary, long-term, or permanent suspension of user privileges. The District will cooperate with law enforcement in investigating any unlawful actions. The Superintendent or designee has the authority to sign any criminal complaint on behalf of the District.

Any attempted violation of District policies, procedures, or other rules will result in the same consequences, regardless of the success of the attempt.

Legal References:

15 U.S.C. §§ 6501-6506, Children's Online Privacy Protection Act (COPPA)
20 U.S.C. § 1232g, Family Educational Rights and Privacy Act (FERPA)
20 U.S.C. § 1232h, Protection of Pupil Rights Amendment (PPRA)
20 U.S.C. § 1400-1417, Individuals with Disabilities Education Act (IDEA)
20 U.S.C. § 7926, Elementary and Secondary Education Act (ESSA)
RSA 31:103-b, Cybersecurity
RSA 189:65, Definitions
RSA 189:66, Data Inventory and Policies Publication
RSA 189:67, Limits on Disclosure of Information
RSA 189:68, Student Privacy
RSA 189:68-a, Student Online Personal Information
RSA 359-C:19-21, Right to Privacy/Notice of Security Breach

Additional Resources:

N.H. Dept. of Education Minimum Standards for Privacy and Security of Student and Employee Data: https://www.education.nh.gov/sites/g/files/ehbemt326/files/inline-documents/minimum-standards-privacy.pdf *(Link as of 2022.8.1)*

(Adopted: 8/5/2019)
(Revised: 3/6/20323)

NHSBA sample policy. Policy Committee suggests replacing current GSD policy with this sample policy.
11-17-2023 Policy Committee
12-4-2023 First Reading
12-6-2023 Sent to GEA
1-8-2024 Second Reading

EHAB

DATA GOVERNANCE AND SECURITY

To accomplish the District's mission and comply with the law, the District must collect, create and store information. Accurately maintaining and protecting this data is important for efficient District operations, compliance with laws mandating confidentiality, and maintaining the trust of the District's stakeholders. All persons who have access to District data are required to follow state and federal law, District policies and procedures, and other rules created to protect the information.

The provisions of this policy shall supersede and take precedence over any contrary provisions of any other policy adopted prior to the date of this policy.

A. Definitions

Confidential Data/Information - Information that the District is prohibited by law, policy, or contract from disclosing or that the District may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information (i.e., "PII") regarding students and employees.

Critical Data/Information - Information that is determined to be essential to District operations and that must be accurately and securely maintained to avoid disruption to District operations. Critical data is not necessarily confidential.

Cybersecurity Incident – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information processes, stores, or transmits, if that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

B. Data and Privacy Governance Plan - Administrative Procedures.

1. Data Governance Plan. The Superintendent, in consultation with the District Information Security Officer ("ISO") (see paragraph C, below), shall update the Data and Privacy Governance Plan ("Data Governance Plan") for presentation to the Board annually.

   The Data Governance Plan shall include:

   a. An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher,

privacy statement, and terms of use;

b. A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed minimum standards set by the New Hampshire Department of Education;

c. Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools, and extensions used on District hardware, server(s) or through the District network(s);

d. A response plan for any breach of information/cybersecurity incidents; see RSA 31:103-b and RSA 359-C:19-21;

e. A requirement for a service provider to meet or exceed standards for data protection and privacy; and

f. A provision that students participating in career exploration or career technical education may, with written parental consent, register for technology platforms and services to be used as part of the student's approved program of study, which require the provision of personally identifiable information. Copies of written parental consent shall be retained as part of a student's educational record.

g. and provisions that meet or exceed the standards set forth in the N.H. Dept. of Education's *Minimum Standards for Privacy and Security of Student and Employee Data.*

2. Policies and Administrative Procedures. The Superintendent, in consultation with the ISO, is directed to review, modify, and recommend (policies) create (administrative procedures), where necessary, relative to collecting, securing, and correctly disposing of District data (including, but not limited to Confidential and Critical Data/Information, and as otherwise necessary to implement this policy and the Data Governance Plan. Such policies and/or procedures may or may not be included in the annual Data Governance Plan.

C. Information Security Officer.

The Director of Technology is hereby designated as the District's Information Security Officer (ISO) and reports directly to the Superintendent or designee. The ISO is responsible for implementing and enforcing the District's security policies and administrative procedures applicable to digital and other electronic data, and suggesting changes to these policies, the Data Governance Plan, and procedures to better protect the confidentiality and security of District data. The ISO will work with both the District and building level administrators and Data managers (paragraph E, below) to advocate for resources, including training, to best secure the District's data.

The IT Support Coordinator is the District's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

D. Responsibility and Data Stewardship.

All District employees, volunteers and agents are responsible for accurately collecting, maintaining, and securing District data including, but not limited to, confidential and/or critical data/information.

E. Data Managers.

All District administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the District's data inventory. Data managers will monitor employee access to the information to ensure that confidential information is accessed only by employees who need the information to provide services to the District and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISO in enforcing District policies and procedures regarding data management.

F. Confidential and Critical Information.

The District will collect, create or store confidential information only when the Superintendent or designee determines it is necessary, and in accordance with applicable law. The District will provide access to confidential information to appropriately trained District employees and volunteers only when the District determines that such access is necessary for the performance of their duties. The District will disclose confidential information only to authorized District contractors or agents who need access to the information to provide services to the District and who agree not to disclose the information to any other party except as allowed by law and authorized by the District.

District employees, contractors and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise.

The Superintendent and/or the ISO shall immediately report any known or suspected cybersecurity incidents within the District's information systems, or within an information system of any vendor of the District, to the New Hampshire Cyber Integration Center of the Department of Information Technology. The Superintendent and/or the ISO shall disclose all known information and interactions. See RSA 31:103-b.

The ISO or designee will investigate immediately and take any action necessary to secure the information, issue all required legal notices and prevent future incidents. When necessary, the Superintendent, ISO, or designee is authorized to secure resources to assist the District in promptly and appropriately addressing a security breach.

As a part of this investigation, the ISO or designee will promptly determine the likelihood that any information part of a cybersecurity incident has been or will be misused. If the determination is that the misuse of information has occurred or is reasonably likely to occur, or if a determination cannot be made, the ISO will notify the affected individuals as soon as possible, consistent with the notification requirements under RSA 359-C:20.

Likewise, the District will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure.

All District staff, volunteers, contractors, and agents who are granted access to critical or confidential information/data are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of such confidential or critical data/information. All individuals using confidential and critical data/information will strictly observe all administrative procedures, policies, and other protections put into place by the District including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information no longer needed in a confidential and secure manner.

G. Using Online Services and Applications.

District staff members are encouraged to research and utilize online services or applications to engage students and further the District's education mission. District employees, however, are prohibited from installing or using applications, programs or other software, or online system/website, that either stores, collects, or shares confidential or critical data/information, until the ISO approves the vendor and the software or service used. Before approving the use or purchase of any such software or online service, the ISO or designee shall verify that it meets the requirements of the law, Board policy, and the Data Governance Plan, and that it appropriately protects confidential and critical data/information. This prior approval is also required whether or not the software or online service is obtained or used without charge.

Notwithstanding the prohibition on the use of applications, etc. that store, collect or share personally identifiable information concerning a student ("PII"), students participating in career exploration or career technical education may, with written parental consent**,** register for technology platforms and services to be used as part of the student's approved program of study, even if said platforms and services require the collection, storage and sharing of the student's PII. Use of these platforms and services is subject to the conditions set forth in B.1(f), above, and related provisions of the Data Governance Plan. The written parental consent forms shall be retained as student records.

H. Training.

The ISO will provide appropriate training to employees who have access to confidential or critical information to prevent unauthorized disclosures or breaches in security. All school employees will receive annual training in the confidentiality of student records, and the requirements of this policy and related procedures and rules.

I. Data Retention and Deletion.

The ISO or designee shall establish a retention schedule for the regular archiving and deletion of data stored on District technology resources. The retention schedule should comply with, and be incorporated into the data/record retention schedule established under Board policy EHB and administrative procedure EHB-R, including but not limited to, provisions relating to Litigation and Right to Know holds as described in Board policy EHB.

J. Consequences

Employees who fail to follow the law, or District policies or procedures, regarding data governance and security (including failing to report) may be disciplined, up to and including termination. Volunteers may be excluded from providing services to the District. The District will end business relationships with any contractor who fails to follow the law, District policies or procedures, or the confidentiality provisions of any contract. In addition, the District reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

The District may suspend all access to data or use of District technology resources pending an investigation. Violations may result in temporary, long-term, or permanent suspension of user privileges. The District will cooperate with law enforcement in investigating any unlawful actions. The Superintendent or designee has the authority to sign any criminal complaint on behalf of the District.

Any attempted violation of District policies, procedures, or other rules will result in the same consequences, regardless of the success of the attempt.

Legal References:

15 U.S.C. §§ 6501-6506, Children's Online Privacy Protection Act (COPPA)
20 U.S.C. § 1232g, Family Educational Rights and Privacy Act (FERPA)
20 U.S.C. § 1232h, Protection of Pupil Rights Amendment (PPRA)
20 U.S.C. § 1400-1417, Individuals with Disabilities Education Act (IDEA)
20 U.S.C. § 7926, Elementary and Secondary Education Act (ESSA)
RSA 31:103-b, Cybersecurity
RSA 189:65, Definitions
RSA 189:66, Data Inventory and Policies Publication
RSA 189:67, Limits on Disclosure of Information
RSA 189:68, Student Privacy
RSA 189:68-a, Student Online Personal Information
RSA 189:70 Educational Institution Policies on Social Media
RSA 359-C:19-21, Right to Privacy/Notice of Security Breach

Additional Resources:

N.H. Dept. of Education Minimum Standards for Privacy and Security of Student and Employee Data: https://www.education.nh.gov/sites/g/files/ehbemt326/files/inline-documents/minimum-standards-privacy.pdf *(Link as of 2022.8.1)*

NHSBA sample policy. We do not have this policy. The Policy Committee recommends adopting this policy.

11-17-2023 Policy Committee

12-4-2023 First Reading

12-8-2023 Sent to GEA

1-8-2024 Second Reading

EBCC

False Alarms, Bomb, Active Shooter and Other Such Threats

The Board recognizes that false alarms, and bomb, active shooter or other such violent threats, are a significant concern to schools. Whether a threat is real or a hoax, it represents a likely substantial disruption to the educational mission of the school, as well as potential danger to the safety and welfare of students, staff, and school property.

No person shall make or communicate, by any means, a threat stating the current or future presence of: a fire, an explosion, an active shooter, an explosive device, a biological or chemical substance, or other catastrophic emergency on school premises. This prohibition extends to activating any alarm on school property intended to warn of the presence of one or more such threats or conditions when the person activating the alarm knows the threat or condition is not present, or there is no reasonable basis presence of such threat or condition. Making such threats or false alarms will be deemed a violation of the applicable code of conduct, with potential disciplinary action, and will be referred to law enforcement for potential criminal prosecution.

Any such false threat or alarm will be regarded as a serious matter and will be treated accordingly. In the event a violent threat is made or alarm activated, the Building Principal/supervisor shall follow the pertinent procedures set forth in the District Crisis Prevention and Response Plan EBCA, and the school specific Emergency Operations Plan. At a minimum:

1. The Superintendent or designee shall**,** in collaboration with local law enforcement, make a determination as to whether an immediate evacuation of school buildings is required in accordance with the District Crisis Prevention and Response Plan.

2. An investigation of the threat should be made by local law enforcement authorities or applicable state department.

3. Any decision to re-enter the school or buildings after an evacuation will be made by the Superintendent, or designee, and only after such clearance has been given by the appropriate law enforcement agency.

4. The Superintendent or designee will communicate the occurrence of any threat under this policy to the parents of any students in the affected building, whether or not a full evacuation occurred either in accordance with the District Crisis Prevention and Response Plan or the District Communication Plan or as soon as deemed appropriate under the circumstances.

Legal References:

NH Statutes	Description
RSA 158:9	Possession of Explosives
RSA 644-a	False Fire Alarms
RSA 644:3	False Public Alarms

NHSBA Sample Policy. We do not have this policy. It is referred to in policy FAA and recommended by the Policy Committee.

11-17-2023 Policy Committee

12-4-2023 First Reading

12-8-2023 Sent to GEA

1-8-2024 Second Reading

FA

FACILITIES DEVELOPMENT GOALS AND PREPARATION OF CAPITAL IMPROVEMENT PLAN

A. **Policy Statement.** As the Board seeks to incorporate the most appropriate and cost-effective risk management techniques for loss prevention and control, and to overcome deficiencies in its physical plant, it will strive to provide new and remodeled facilities that will offer the best possible physical environment for learning and teaching. The Board specifically recognizes the need and importance of regular and substantial capital maintenance, renovation, improvement and expansion consistent with realistic fiscal constraints.

B. **Facility Considerations, Goals and Objectives.** In establishing specific facility plans, the Board will use the following considerations, goals and objectives among others:

1. Facilities, including buildings, ground, and playing fields, that will accommodate organization and instructional patterns that support the district's educational philosophy and instructional goals.

2. Meeting all safety requirements through the remodeling and renovation of older structures.

3. Providing building renovations to meet requirements on the availability of public school facilities to meet ADA compliance whenever possible.

4. Building designs, construction, and renovations that will lend themselves to low maintenance costs and the conservation of energy.

5. Facilities that will also lend themselves to utilization by the community in ways consistent with the overall goals of the district.

6. Keeping the community informed about the condition of district facilities as well as the perceived needs in the areas of capital improvement expansion and acquisition.

7. Decisions pertaining to education specifications of new buildings and those undergoing extensive remodeling will be developed with the input of teachers, students, parents, and the community.

C. **Capital Improvement Program.** The Superintendent or designee will prepare and update a long-range capital improvement program, to be reviewed at least every 2 years, that identifies District school facility goals, provides projected expenditures, and outlines procedures and guidelines to be followed to accomplish Board and District goals. This program will be provided to the Department of Education pursuant to RSA 198:15-a, so that the state can project funds needed for building projects occurring in the District and elsewhere.

NH Statutes	**Description**
RSA 198:15-a	Grant for School Construction

Current GSD Policy. The Policy Committee suggests replacing with NHSBA sample policy to comply with HB536.
11-17-2023 Policy Committee
12-4-2023 First Reading
12-8-2023 Sent to GEA
1-8-2024 Second Reading

ANNUAL FACILITY PLAN

A. Drafting and Adoption. Each year, the School Board shall adopt an updated Facility Plan. The first Facility Plan shall be adopted no later than June 1, 2022, with an updated plan approved by the Board by June 1 of 2023 and each year thereafter.

The Facility Plan shall be developed and drafted by the Superintendent or his/her designee, and it shall be proposed to the School Board for comment and adoption at least 30 days prior to the adoption deadlines articulated above.

B. Contents of Facility Plan. The Facility Plan shall account for each facility owned by the District and document the use of each such facility. For each then unused facility, the plan shall specify any uses intended within the next two years of the annual plan approval relative to academic purposes, extracurricular activities, administrative functions, and/or sports. Facilities for which no current or intended use is included on the plan shall be referred to in this policy as "Unused Facilities".

C. Annual Report to N.H. Department of Education. The Superintendent shall submit a report of Unused Facilities to the New Hampshire Department of Education, with the first such report due January 1, 2022 and subsequent reports due July 1 each year thereafter. Pursuant to RSA 194:61, such Unused Facilities are then encumbered by a right of first refusal ("ROFR") available to every approved charter school operating in New Hampshire. The specifics of the ROFR are described in RSA 194:61, III-VII.

(Adopted: 3/8/2022)

NHSBA Sample Policy. The Policy Committee recommends replacing current GSD policy with this sample policy to comply with HB536.
11-17-2023 Policy Committee
12-4-2023 First Reading
12-8-2023 Sent to GEA
1-8-2024 Second Reading

ANNUAL FACILITY PLAN AND UNUSED DISTRICT PROPERTY FAA

A. **Drafting and Adoption.** Thee School Board shall adopt and approve an Annual Facility Plan by June 1 of each year.

The Facility Plan shall be developed and drafted by the Superintendent or designee and it shall be proposed to the School Board for comment and adoption at least 30 days prior to the adoption deadline articulated above.

B. **Contents of Facility Plan.** In preparing the annual Facility Plan, due consideration will be given to the most recent Capital Improvement Program prepared pursuant to Board policy FA. The Facility Plan shall account for each facility owned by the District and document the use of each such facility. For each then unused facility, the plan shall specify any uses intended within the next two years of the annual plan approval relative to academic purposes, extracurricular activities, administrative functions, and/or sports. Facilities for which no current or intended use is included on the plan shall be referred to in this policy as "Unused Facilities".

C. **"Unused Facility" Defined.** As used in the policy, "Unused Facility" or "Unused Facilities" shall mean any district owned school building which is not currently used for academic purposes, extracurricular activities, administrative school functions, or sports, and for which the School Board has not approved a written plan for future use.

D. **Annual Report to N.H. Department of Education.** The Superintendent shall submit a report of Unused Facilities to the New Hampshire Department of Education no later than July 1 of each year.

E. **Charter School Rights Relative to Unused Facilities.**

1. Right of First Refusal: Pursuant to RSA 194:61, such Unused Facilities are encumbered by a right of first refusal ("ROFR") available to every approved charter school operating in New Hampshire. If the District has an Unused Facility which it seeks to sell or lease to a party other than an approved charter school, the District will include a ROFR provision in the offer for sale/lease and/or a sale/lease contract.

2. Conditional Contract for Sale/Lease. If a prospective purchaser which is not an approved charter school enters into a contract with the District for purchase, lease or sale, (that is, an offer to sell/lease by the District is accepted by the prospective purchaser), the contract (the "Original Contract") will be conditioned upon the expiration of the ROFR**.** It is essential that the prospective purchaser or lessee is made aware of the ROFR prior to execution of the Original Contract, and that the

Original Contract clearly articulate the ROFR with specific reference to RSA 194:61. The District will promptly notify the Charter School Administrator of the Department of Education ("DOE Charter School Administrator") in order for the Department to alert all approved charter schools in the state and allow them a chance to respond. The notice provided to the DOE Charter School Administrator shall contain clear language that the Unused Facility is available to any approved chartered public school in this state only, and shall list the offering school district's name and location, the square footage of the Unused Facility, the contact information of the offering school district's representative, and the expiration date of the right of first refusal which shall be 60 days after the date of the date the District provides notice to the DOE Charter School Administrator.

3. Charter School Rights if No Other Offer Received. If the offering school district has not received an offer to purchase or lease an Unused Facility from a party, other than an approved chartered public school operating in this state, a chartered public school may initiate, and Board shall engage in, good faith negotiations for the purchase or lease of the Unused Facility.

4. Invocation of Rights by One or More Approved Charter Schools. If the District receives an offer on an Unused Facility from an approved charter school prior to the expiration date of the ROFR, the District will respond promptly to the offer and notify the prospective purchaser under the Original Contract and engage in good faith negotiations. If more than one chartered public school makes an offer on the District's Unused Facility, the School Board will make the final selection between the parties based on criteria established by the School Board and in accordance with the best interests of the District.

5. Procedure for Resolution of Negotiation Impasse. A chartered public school that makes an offer shall have 6 months after the date of making a written offer to complete the purchase or lease of the Unused Facility for a price which the District has agreed upon.

6. District Discretion. In right of first refusal negotiations with a chartered public school, it shall be the option of the Board whether to sell or to lease the property under consideration, at fair market value or less, for a term to be agreed upon by the parties. Any lease terms shall include, among others agreed upon by the parties, any required provisions for such leases as found in RSA 194:61.

7. Expiration of Right of Charter School After Written Offer. The chartered public school shall have 6 months after the date of making a written offer to complete the purchase or lease of the unused facility for a price negotiated with the school district.

NH Statutes	**Description**
RSA 194:61	Unused District Facilities