# Concord School District Policy #247
# 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, Board 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 about 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.

**B. Information Security Officer**

The Director of Technology is designated as the District's Information Security Officer (ISO) and reports directly to the Superintendent. The ISO is responsible for implementing and enforcing the Board's security policies, and administrative procedures applicable to digital and other electronic data, and suggesting changes to the Data and Privacy Governance Plan (DGP, see C. below), and procedures to better protect the confidentiality and security of District data.

The System Administrator is the District's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

**C. Data privacy governance and administrative procedures**

1. Data Governance Plan. The Superintendent, in consultation with the ISO, shall create a Data and Privacy Governance Plan to be presented to the Board no later than June 30, 2019. Thereafter, the Superintendent, in consultation with the ISO, shall update the DGP for presentation to the Board no later than June 30 each year. The DGP 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. Procedures for access to data and protection of privacy for students and staff, including acceptable use 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; and

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

2. Administrative procedures. The Superintendent, in consultation with the ISO, will review, modify and recommend administrative procedures 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 DGP). Such procedures will be included in the annual DGP.

**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 Board 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 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 ISO 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 or ISO is authorized to secure resources to assist the District in promptly and appropriately addressing a security breach.

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**

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 any online system/website that 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 shall verify that it meets the requirements of the law, Board policy, and the DGP, 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.

**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 Superintendent 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 **Policy #249 Data/Records Retention**, including but not limited to provisions relating to Litigation and Right to Know holds.

**J. Consequences**

Employees who fail to follow the law or Board 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, Board 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 has the authority to sign any criminal complaint on behalf of the District.

Any attempted violation of Board 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 189:65 Definitions
RSA 186:66 Student Information Protection and Privacy
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
Policy #249 Data/Records Retention

Adopted on December 3, 2018
Corresponds to NHSBA Policy EHAB