EHAB

DATA GOVERANCE AND SECURITY

To accomplish the Rochester School 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.

B. Data and Privacy Governance Plan - Administrative Procedures.

1. Data Governance Plan. The Superintendent, in consultation with the District CTO (Chief Technology Officer) shall create a Data and Privacy Governance Plan ("Data Governance Plan"), to be presented to the Board by June 30, 2019 or when required by law. Thereafter, the Superintendent, in consultation with the CTO, shall update the Data Governance Plan for presentation to the Board no later than June 30 each year or when required by law.

   The Data Governance Plan shall include:

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

   (b) A review of all known software applications, digital tools, and extensions and an assurance that they meet or exceed minimum standards set by the board and any applicable state and federal laws;

   (c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools, etc. used on District Information Technology (IT) systems.;

   (d) A response plan for a breach of information; and

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy as per state or federal law.

2. Policies and Administrative Procedures. The Superintendent, in consultation with the CTO, 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 will may or may not be included in the annual Data Governance Plan.

C. Information Security Officer.

The CTO is hereby designated as the District's Information Security Officer (ISO) and reports directly to the Superintendent or designee. The CTO is responsible oversight of 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 CTO and IT staff will coordinate with the both District and building level administrators and Data managers to advocate for resources, including training, to best secure the District's data.

Key members of the District's IT Staff are the District's alternate ISO and will assume the responsibilities of the CTO when the CTO 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 CTO in providing guidance with adhering to 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 CTO or designee will investigate as soon as possible and recommend any action necessary to secure the information and work with district staff to insure all required legal notices and prevent future incidents. When necessary, the Superintendent, CTO or designee 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.

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.

H. Training.

The District 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 initial and refresher guidelines in the confidentiality of student records, and the requirements of this policy and related procedures and rules.

I. Data Retention and Deletion.

The District shall establish a retention schedule for the regular archiving and deletion of data stored on District technology resources. The retention schedule should comply with existing school board polies and meet or exceed any state and federal legislation.

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.

Board Adopted: February 14, 2019
Review/Amend: November 14, 2019