Contents

Introduction
Security Committee
Purpose
Scope
Regulatory Compliance
Data User Compliance
Data Lifecycle
Identifying Need & Assessing Systems for District Requirements
New Software or Services
Review of Existing Systems
Management and Storage
Data Access
Data Management
Data Classification and Inventory
Security/Protection
Risk Management
Security Logs
Physical Security Controls
Inventory Management
Asset Disposal
Virus, Malware, SPAM Protection and Web Filtering
Authorization and Authorization
Usage and Dissemination
Data Storage and Transmission
Training
Archival and Destruction
Critical Incident Response
Disaster Recovery
Data Breach Response
Appendix A - Definitions
Appendix B - Laws, Statutory, and Regulatory Security Requirements
Appendix C - Digital Resource Acquisition and Use
Appendix D - Data Breach Response Plan
Introduction

The Salem School District (SSD) is committed to protecting our students’ and employees’ privacy by maintaining appropriate privacy and security protections. The privacy and security of this information is a significant responsibility and we value the trust of our students, parents, and employees.

The SSD Data Governance Plan includes information regarding the Security Committee, data and information governance, applicable School Board policies, District procedures, as well as applicable appendices and referenced supplemental resources.

This plan outlines how administrative and instructional activity shall be carried out to ensure the District’s data is accurate, accessible, consistent, and protected. The document establishes who is responsible for information under various circumstances and specifies what procedures shall be used to manage and protect it. Definitions of terminology can be found in Appendix A: Definitions.

The SSD Data Governance Plan shall be a living document. To make the document flexible, details are outlined in the appendices and referenced supplemental resources. This document and any future modifications to this document will be posted on the District’s website.

Security Committee

The SSD has established a standing Security Committee consisting of the following positions: Superintendent, Assistant Superintendent for Business Operations, High School Dean of Students, Middle School Assistant Principal, High School Library Media Specialist, Communications Manager, IT Generalist and the Chief Information Officer (CIO). Members of the Security Committee will act as data stewards for all data under their direction. The CIO will act as the Information Security Officer (ISO). The Assistant Superintendent for Business Operations is the district’s alternate ISO and will assume the responsibilities of the ISO when the ISO is not available. All members of the district administrative team will serve in an advisory capacity as needed.

Purpose

The School Board recognizes the value and importance of a wide range of technologies for a well rounded education, enhancing the educational opportunities, and achievement of students. The SSD provides its students and employees access to technology devices, software systems, network and Internet services to support teaching, learning and administration. All components of technology must be used in ways that are legal, respectful of the rights of others, protective of its users, and that promote the educational and administrative objectives of the SSD.

To that end, the district must collect, create and store confidential information. Accurately maintaining and protecting this data is important for efficient district operations, compliance with laws and policies, and maintaining the trust of district 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.

It is the policy of the SSD that data or information in all its forms (written, electronic, or printed) is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information. All employees and authorized district contractors or agents
using confidential information will strictly observe protections put into place by the district.

**Scope**

The Data Governance Plan, standards, processes, and procedures apply to all students, employees of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. This plan applies to all forms of SSD data and information, including but not limited to:

- Hard copy data printed or written
- Communications sent by post/courier, fax, electronic mail, text, or any other electronic format
- Data stored and/or processed by any electronic device, including servers, computers, tablets, mobile devices
- Data stored on any type of internal, external, or removable media or cloud based services
- Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems, assets or resources

**Regulatory Compliance**

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix B: Laws, Statutory, and Regulatory Security Requirements).

**Data User Compliance**

The Data Governance Plan applies to all users of SSD information including: employees, students, volunteers, and authorized district contractors or agents. All data users are to maintain compliance with School Board Policies and District administrative procedures including, EHAA (Technology Responsible Use), EHAB (Data Governance and Security Policy) and all policies, procedures, and resources as outlined within this Data Governance Plan and School Board Policy.

A consistently high level of personal responsibility is expected of all users granted access to the district’s technology resources. Any violation of district policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the district’s technology resources. 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.

Unless permission has been granted by the ISO or designee, no employee, vendor or other person may remove confidential or critical data from the district's premises or the district's network, remove a device containing confidential or critical data from the district's premises, or modify or copy confidential or critical data for use outside the district. If permission is given, the data may be accessed only on a district-provided device with appropriate security controls or through a secure virtual private network (VPN). When users access confidential or critical data from a remote location, the user must take precautions to ensure that the confidential or critical data is not downloaded, copied or otherwise used in a manner that would compromise the security and confidentiality of the information.

Employees who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined or terminated. Volunteers may be excluded from providing services to the district. The district may 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 revocation of an employee’s teaching certificate. Any attempted violation of district policies, procedures or other rules may result in the same consequences, regardless of the success of the attempt.

Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of Personally Identifiable Information (PII) or Confidential Information
- Unauthorized copying of district data containing PII or Confidential Information
- Unauthorized sharing user IDs or passwords
- Applying for a user ID under false pretenses or using another person’s ID or password
- Unauthorized use of an authorized ID and password to examine records or information for which there has been no approval
- Attempting to secure a higher level of privilege without authorization
- Installation of software or use of online services not approved
- Unauthorized altering, destruction, or disposal of district information, data and/or systems

Data Lifecycle

Data Governance is necessary at each phase in the data lifecycle. This lifecycle starts at evaluating the need for data collection and ends when the data is destroyed. It is important that appropriate safeguards, policies, procedures and practices are in place for each phase of the data lifecycle.

Identifying Need & Assessing Systems for District Requirements

To accomplish the district’s mission and to comply with the law, the district may need to maintain confidential information, including information regarding students, employees, parents/guardians, applicants for employment and others. The district will collect, create or store confidential information only when the Superintendent or designee determines it is necessary.

New Software or Services

District employees 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. 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 required whether or not the software or online service is obtained or used without charge.
Employees are required to complete steps outlined under the Staff Resources section of the District’s Student and Employee Data Privacy website, to ensure that all new resources meet business and/or instructional need as well all applicable laws and policies.

Memorandums of understanding (MOU), contracts, terms of use and privacy policy for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation. (see Appendix C: Digital Resource Acquisition and Use).

A current list of all vetted and approved software systems, tools and applications is published on the SSD Student and Employee Data Privacy website.

**Review of Existing Systems**

The District will ensure that data collection is aligned with School Board Policy EHAB. Data systems shall be regularly reviewed to ensure that only necessary data is being collected.

Student and employee data is submitted to approved service providers in order to support administrative operations and instructional services. At times, these submissions include PII. The District will ensure that each piece of PII is necessary for operations or instruction and that the providers are abiding by district Data Privacy Agreement.

**Management and Storage**

**Data Access**

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. Such access needs to be reviewed and approved by the ISO.

**Data Management**

The effective education of students and management of district personnel often require the district to collect information, some of which is considered confidential by law and district policy. In addition, the district maintains information that is critical to district operations and that must be accurately and securely maintained to avoid disruption to district operations.

Data Managers are responsible for the oversight of practices and procedures to ensure the security and accuracy of data. 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. Data managers will:

- Ensure that account creation and data access on instructional and administrative systems appropriately match employee’s job function
- Ensure that employees are trained in the district’s proper procedure and practices in order to ensure accuracy and security of data
- Assist the ISO in enforcing district policies and procedures regarding data management
Data Classification and Inventory

Classification is used to promote proper controls for safeguarding the confidentiality of data. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data is classified according to the most sensitive detail they include. Data recorded in several formats (e.g., source document, electronic record, report) have the same classification regardless of format.

The ISO or designee will identify all systems containing district data, such as student information systems, financial systems, payroll systems, transportation systems, food-service systems, email systems, instructional software applications and others. To the extent practical, the ISO or designee will identify the data files and data elements maintained in those systems and identify confidential and critical information the district possesses or collects. Once the data files and data elements are identified, the ISO or designee will classify the data as confidential or critical. Note - This is a complicated process and will happen over time.

The district will create and maintain a data inventory for all information systems containing PII or confidential information. When possible, a data dictionary will be maintained for critical information systems. The data inventory may contain the following elements:

- Data source
- What data is stored
- Where the data is stored
- Person(s) assigned to manage the data
- Employee or employee categories that have access to the data
- When the data is collected and received
- Criticality/Sensitivity Rating

Security/Protection

Risk Management

A risk analysis of SSD data networks, systems, policies, and procedures will be conducted periodically by an external third party or as requested by the Superintendent, ISO or designee. The risk analysis will be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Security Logs

The District will maintain a comprehensive list of critical system events that will be logged and monitored to ensure data reliability and security. These events will include, but are not limited to, access to critical systems and modification of critical data. When applicable, notifications will be established for critical event triggers.

Physical Security Controls

Technology closets (where all core server, networking and telecommunications equipment is kept) exist in every district building and must be kept secure. Access authorization must be approved by the CIO or Director of Facilities. Servers and/or storage (including filing cabinets) containing PII or Confidential information shall be secured in manner to prevent theft, destruction, or access by unauthorized individuals.
Inventory Management

Major technology devices or systems, considered an asset, are inventoried and verified through a regular inventory verification process by the technology department. This includes, but is not limited to, network equipment, servers, computers, laptops, web filters, firewalls, and classroom AV technology.

Asset Disposal

The CIO shall approve disposal (recycle, sale or donation) of any district technology asset. The district will ensure that all assets containing PII, confidential, or internal information are disposed of in a manner that ensures that this information is destroyed. In addition, software licenses are not transferred outside the district. Therefore, systems that are sold or donated will have the hard drive completely wiped.

Malware, SPAM Protection and Web Filtering

The District uses a multi-layered approach to protect electronic data. This includes, but is not limited to, secure DNS, firewalls, SPAM filter, Advanced Threat Protection, antivirus, anti-malware, anti-spyware, anti-ransomware software, and group policies. In compliance with The Children’s Internet Protection Act (CIPA) and to provide an appropriate online experience, the district also employs web filtering. Users shall not turn off or in any way impede or attempt to circumvent the function of these systems.

Authentication and Authorization

District employees will only access personally identifiable and/or confidential information if necessary to perform their duties. The district will only disclose this information 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.

Mechanisms to control access to PII, confidential information, internal information and computing resources include, but are not limited to:

- Authentication: Unique user identification (user ID) for authentication is required for all systems that maintain or access PII, confidential information, and/or internal information. Users are held accountable for all actions performed on the system with their User ID. User IDs and passwords must not be shared.
- Authorization: Access controls are maintained through a partnership between the technology department, human resources (HR) and data managers to ensure access is limited to what is necessary for job performance.

Only members of the District Technology staff will be granted elevated access to systems in order to perform their job functions. In special circumstances, and with the approval of the ISO, employees may be granted elevated access to their district assigned device or devices they are responsible for.

Employees

Notification of a new employee is sent from Human Resources to the Technology Department. This notification includes person replacing (if applicable), role, building assignment(s), and start date. After notification has been received from Human Resources, the Technology Department will create employee user IDs. Each employee will be given access and permissions to the necessary resources based on their position.

Students

Notification of a new student is sent from one of the registrars to the Technology Department. After
notification has been received from a registrar, the Technology Department will create a student user ID.

**Contractors/Vendors**

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor data access must be approved by an administrator and the ISO. All contractors/vendors accessing district data will be considered on premise users. Once the approval has been obtained, the technology department will create the account, only granting access to the server/application that the contractor/vendor supports.

**Account Deletion**

Student and employee accounts are disabled as soon as the Technology Department is notified of separation, or upon graduation in the case of high school seniors. Contractor/Vendor accounts are deleted when the data manager notifies the Technology Department that the business relationship or need for access no longer exists.

**Password Security**

The District will enforce secure passwords for all systems within their control. All passwords to district systems shall; be a minimum of 8 characters, include a capital and number. Users must adhere to the following behaviors relative to their passwords:

-Passwords should never be shared with another person
-Passwords should never be written on paper or affixed to the user’s device
-Passwords should not be ones that are easily guessed due to their association with the user (i.e. children’s names, pets’ names, or birthdays)
-Employees are required to change their password at least annually
-Users who have reason to believe a password is lost or compromised must notify the CIO or designee immediately

**Session Control**

When possible, the district will limit the number of concurrent sessions for a user ID on a system. Session timeouts will be implemented on all systems containing PII.

**Remote Access**

Employee direct access into the District’s network from outside is strictly prohibited without explicit authorization from the ISO. Access will be provided through a virtual private network (VPN) connection through the district’s firewall. No other method of remote access shall be granted without explicit authorization from the ISO.

In the event that VPN access is needed by a contractor/vendor, access must be approved by the appropriate data manager and ISO. The IT Generalist will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

**Usage and Dissemination**

All users are responsible for the security and integrity of the data they create, store or access. Users are expected to act as good stewards of data and treat data security and integrity with a high degree of responsibility and priority.

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.

District data security applies to all forms of data, including data stored on devices, data in transit and data stored on additional resources.

**Data Storage and Transmission**

Employees and students are provided two forms of system-based data storage for their individual files, Google Drive and local storage on district servers. Access to these is restricted to the folder’s owner (employee or student who is assigned).

No other systems can be used by employees, to store district data, without the permission of the ISO. This includes, but is not limited to alternative cloud services and external storage devices (including USB drives, rewritable CD/DVD, memory cards, and external hard drives).

**File Transmission Practices**

Employees are responsible for securing sensitive data for transmission through email or other channels. Employees should not transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval. When possible, staff should de-identify or redact any PII or confidential information prior to transmission. Regular transmission of student data to district-approved services is managed by the technology department using a secure data transfer protocol.

**Credit Card and Electronic Payment**

Employees can only use those systems approved by the ISO to process electronic payments, including, but not limited to, processing credit card information. All cardholder data may only be entered in secured payment systems approved by the district. Any cardholder data collected in written form must be shredded immediately after entry into approved system. The following guidelines should be followed when handling payment information:

- Payment information will be stored and processed by a 3rd party accessible through a secure portal
- No request for cardholder information will be transmitted via email or any other electronic communication system
- Payment information shall be entered directly into the approved payment system by the individual making payment. If the individual is not able to directly input the payment, designated staff may gain verbal approval for the payment process either in person or via phone (after identification is verified). If verbal payment information is received, that information must be entered directly into the payment system and not written down during the process.
- If payment information is collected via a physical form, that form must be shredded or payment information redacted immediately upon receipt and entry into payment system

**Mass Data Transfers**

Downloading, uploading or transferring PII, confidential information, and internal information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be in reviewed and approved by the Superintendent or designee. All other mass downloads of information shall be approved by the ISO and include only the minimum amount of information necessary to fulfill the request.
Printing

When possible, staff should de-identify or redact any PII or confidential information prior to printing. PII and confidential information shall not be copied or printed indiscriminately or left unattended and open to compromise. When printing PII or confidential information is necessary, it is strongly recommended that users use the secure printing function.

Training.

The district shall create and maintain a data security training program. This program will consist of the following, at a minimum:

- Training for all employees on applicable technology laws, policies and procedures, including confidentiality and data privacy
- Training for all employees on applicable federal regulations and the use of digital resources and student electronic records
- Training for district administrators on their responsibilities as data managers for the data they are responsible for
- Training or professional learning, that includes the use of PII data, shall include reinforcement on data security

Archival and Destruction

Once data is no longer needed, the ISO or designee will work with the data manager to ensure that it is appropriately destroyed. Special care will be taken to ensure that confidential information is destroyed appropriately and in accordance with law. Confidential paper records will be destroyed using methods that render them unreadable, such as shredding. Confidential digital records will be destroyed using methods that render the record unretrievable.

Critical Incident Response

Controls shall ensure that the District can recover from any damage to or breach of critical systems, data, or information within a reasonable period of time. The District shall maintain a list of all critical systems and data, including contact information.

Each school, department, or individual is required to report any instances immediately to the ISO or designee for response to a system emergency or other occurrence (for example, fire, vandalism, system failure, data breach and natural disaster) that damages/breaches data or systems.

Disaster Recovery

The CIO will develop a district Technology Disaster Recovery Plan which will be added to this Data Governance Plan as an appendix. At a minimum, the plan will outline critical staff, responsibilities, and processes in the event of a disaster or critical data loss.

Data Breach Response

New Hampshire’s data breach law is triggered when a School District computer system is breached and
personal information (RSA 359-c:19, IV (a)) is acquired without authorization in a way that compromises the security or confidentiality of the information. The law requires a school district, experiencing a breach, to conduct a good faith and reasonably prompt investigation to determine the likelihood that personal information was, or will be, misused (RSA 359-c:20, I (a)). The Data Breach Response Plan enables the District to respond effectively and efficiently to a data breach involving personally identifiable information (PII) as defined by NH Law, confidential or protected information, district identifiable information and other significant cybersecurity incident. The Data Breach Response Plan shall include processes to validate and contain the security breach, analyze the breach to determine scope and composition, minimize impact to the users, and provide notification (see Appendix D: Data Breach Response Plan).
Appendix 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 (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.

Data Breach, Breach of Security or Breach: A security incident in which there was unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information.

Data Integrity: Data is current, accurate and has not been altered or destroyed in an unauthorized manner.

Data Management: The development and execution of policies, practices, and procedures in order to manage the accuracy and security of district instructional and administrative data in an effective manner.

Data Owner: User responsible for the creation of data. The owner may be the primary user of that information or the person responsible for the accurate collection/recording of data. Ownership does not signify proprietary interest, and ownership may be shared.

Information Security Officer: The Information Security Officer (ISO) is responsible for working with the Superintendent, Security Committee, data managers, data owners, and users to develop and implement prudent security policies, procedures, and controls.

Systems: Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, server, internal or external storage, communication device or any other current or future electronic or technological device, whether hosted by the district or provider.

Security Incident: An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2) constitutes a violation or imminent threat of violation of security policies, security procedures or responsible-use policies.

Personally Identifiable Information (PII): Data elements as defined in section VII & VII-a of NH RSA 189:65.

Risk: The probability of a loss of confidentiality, integrity, or availability of information resources.

User: Any person who has been authorized to read, enter, print or update information.
Appendix B - Laws, Statutory, and Regulatory Security Requirements

**CIPA:** The Children’s Internet Protection Act was enacted by Congress to address concerns about children’s access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

**COPPA:** The Children’s Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children.

**FERPA:** The Family Educational Rights and Privacy Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.

**HIPAA:** The Health Insurance Portability and Accountability Act applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.

**PPRA:** The Protection of Pupil Rights Amendment affords parents and minor students’ rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.

**New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data:** A set of standards created by the New Hampshire Department of Education. These are a subset of the National Institute of Standards and Technology (NIST) created by the US Department of Commerce.

**New Hampshire State RSA 189:65-189:68:** Student and Teacher Information Protection and Privacy as defined by the following sections:

- NH RSA 189:65 Definitions
- NH RSA 189:66 Data Inventory and Policies Publication
- NH RSA 189:67 Limits on Disclosure of Information
- NH 189:68 Student Privacy
- NH RSA 189:68-a Student Online Personal Information

**New Hampshire State RSA Chapter 359-C Right to Privacy:** Data breach guidelines.
- NH RSA 359-C:19 Notice of Security Breach - Definitions
- NH RSA 359-C:20 Notice of Security Breach Required
- NH RSA 359-C:21 Notice of Security Breach Violation
Appendix C - Digital Resource Acquisition and Use

The purpose of the Digital Resource Acquisition and Use process is:

- Adherence to district, state and federal laws and policies
- Alignment with district curriculum and administrative goals

New Resource Acquisition

Employees must adhere to the following guidelines regarding digital resource acquisition. This includes, but is not limited to, any site or tool that a student or employee uses where they may be creating content online and/or that requires user login.

1. Confer with one of the District Technology Integrators (for academic resources) or the CIO (for administrative resources) to help evaluate the need. There may be an existing tool or resource that can be used or there may be a simple change in process that can accommodate the need.

2. Complete the online request form in the Staff Resources section of the District’s Student and Employee Data Privacy website.

Once the online form is completed:

1. The appropriate Curriculum or Administrative Director will review the request to ensure alignment with District learning or administrative objectives.

2. If approved by the Director, a database will be required to see if the resource was previously vetted for NH State compliance. If yes, we will move forward with the acquisition. If not, then the request will be forwarded to legal counsel for review to ensure regulatory compliance.

District Digital Resources

To meet regulatory requirements and to provide an online inventory, a list of approved digital resources will be maintained on the District’s Student and Employee Data Privacy website.

Digital resources that are not approved or have not yet been reviewed are not allowed to be used by members of the district.

Digital Resource Licensing/Use

Digital resources licensed or purchased for district use are the property of the District and shall not be copied or shared with others outside of the District without prior approval. District members must adhere to the following guidelines regarding digital resource licensing/use:

- Only approved district resources can be used
- Software installed on District systems or services used will have a current license/contract on file in the Technology or Business Office or will be removed from service
- Employees cannot act as a parental agent when creating student accounts for online resources. Resources requiring this permission must be approved by the CIO or designee.
Appendix D - Data Breach Response Plan

Objective

The purpose of the Technology Data Breach Plan (TDBP) is to enable the SSD to respond effectively and efficiently to an actual or suspected data breach involving personally identifiable information (PII), confidential or protected information, or other significant cybersecurity incident.

Incident Response Team

The SSD has appointed the following people to the Incident Response Team (IRT): ISO, IT Generalist and the Assistant Superintendent of Business Operations. The ISO will act as the response manager with the Assistant Superintendent of Business Operations taking the role if the ISO is not available. In the event the TDBP is activated, overall management of the response is delegated to this team.

Activation

The TDBP will be activated if a suspected data breach has occurred where personally identifiable information (PII), confidential or sensitive data has been compromised or a network hack/intrusion has occurred. Once the TDBP is activated, the IRT will convene and:

- Validate and contain the data security breach
- Determine the nature of the data compromised and its impact to users and the district
- Fully document the incident, steps taken to remediate and notify
- Communicate impact, the number of affected individuals, the likelihood information will be or has been used by unauthorized individuals and updates of progress to the Superintendent
- Coordinate all communications through the Superintendent
- Allocate and manage Technology and other District staff resources during the event
- Work with vendors, 3rd party providers, manufacturers, legal counsel, district data breach insurance provider, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Creation of a TDBP debrief report for the Superintendent

Evaluation

Once the breach has been mitigated an internal evaluation of the SSD TDBP response will be conducted. The IRT, in conjunction with others that were involved, will review the breach and all mitigation steps to determine the probable cause(s). Feedback from the responders and affected entities may result in an update to the TDBP and other emergency response plans as appropriate. Changes in security measures and information security training programs will be modified to remediate issues discovered during the response and to minimize the risk of a future occurrence.