School Administrative Unit #6

SAU #6

Claremont & Unity

Data and Privacy Governance Plan

Approved June 2021

Contents

Introduction

SAU #6 is committed to protecting our students' and staffs' privacy through maintaining strong 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 staff.

The Data Governance Plan includes information regarding the data governance team, data and information governance, applicable policies, procedures, as well as applicable appendices and referenced supplemental resources.

This manual outlines how operational 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.

The 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..

Data Governance Team

The Data Governance team consists of the following positions: Superintendent, Assistant Superintendent, Business Administrator, Facilities Director, Human Resources Manager, and the Director of Technology. Members of the Data Governance Team will act as data stewards for all data under their direction. The Director of Technology will act as the Information Security Officer (ISO), with assistance from members of the full Technology team. The Business Administrator 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 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. Faculty, staff, and administrative staff access to technology devices, software systems, network and Internet services to support research and education. All components of technology must be used in ways that are legal, respectful of the rights of others, and protective of juveniles and that promote educational objectives.

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 mandating confidentiality, and maintaining the trust of all 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.

Scope

The data security policy, standards, processes, and procedures apply to all students and staff of the District, contractual third parties and agents of the District, and volunteers who have access to District data systems or data. This policy applies to all forms of data and information, including but not limited to:

- Speech, spoken face to face, or communicated by phone or any current and future technologies.
- Hard copy data printed or written.
- Communications sent by post/courier, fax, electronic mail, text, chat and/or any form of social media.
- 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.
- The terms data and information are used separately, together, and interchangeably throughout the policy, the intent is the same.
- Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV 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.
- All involved systems and information are considered assets of the respective Districts and shall be protected from misuse, unauthorized manipulation, and destruction.

Regulatory Compliance

SAU #6 will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems. SAU #6 complies with the NH Minimum Standards for Privacy and Security of Student and Employee Data. SAU #6 complies with all other applicable regulatory acts including but not limited to the following:

- Children's Internet Protection Act (CIPA)
- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Pupil Rights Amendment (PPRA)
- Individuals with Disabilities in Education Act (IDEA)

- New Hampshire State RSA - Student and Teacher Information Protection and Privacy

    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 Minimum Standards for Privacy and Security of Student and Employee Data (will update link once officially released)
- New Hampshire State RSA - Right to Privacy:

    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

Data User Compliance

The Data Governance Plan applies to all users including: staff, students, volunteers, and authorized District contractors or agents. All data users are to maintain compliance with School Board Policies and District administrative procedures 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.

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.

1. Identify Need
2. Create / Acquire
3. Manage / Store
4. Protect
5. Use / Share
6. Archive

7. Destroy

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, parents/guardians, staff, 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 Systems

District staff members are encouraged to research and utilize online services or applications to engage students and further the District's educational mission. However, before any online service or application is purchased or used to collect or store confidential or critical information, including confidential information regarding students or staff, the ISO or designee must approve the use of the service or application and verify that it meets the requirements of the law and School Board policy and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

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.

All new resources shall be properly evaluated against the following criteria, when applicable:

- Impact on technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract.

Note: Exceptions can be made by the ISO when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent permission is requested from parents during the yearly online registration process for District vetted and approved applications and tools.

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

Review of Existing Systems

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

Individual student level data is submitted to different approved service providers in order to ensure business operations and instructional services. At times, these imports include PII for staff and students. The District must ensure that each piece of PII is necessary for operations or instruction and that the providers are abiding by their terms of service.

Acquisition and Creation

All staff must adhere to the following guidelines regarding a new digital resource acquisition:

- Contracts 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. Staff should speak with their building Technology Integrator before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.
- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets District business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the Assistant Superintendent, Curriculum Specialists and the ISO, or designee, prior to purchase.

Management and Storage

Systems Security

The District will provide access to confidential information to appropriately trained District staff 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. Therefore, system access will only be given on an as-needed basis as determined by the data manager and 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 development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. 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 Classification and Inventory

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. 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. 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 so that those files and the information they contain can be more closely monitored.

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 will contain the following elements:

- Data Source
- What data is stored
- Where the data is stored
- Persons assigned to manage the data
- Staff or staff categories that have access to the files
- When the data is collected and received
- How the data is accessed
- Who has access
- Criticality/Sensitivity Rating

Security/Protection

Risk Management

A thorough risk analysis of all data networks, systems, policies, and procedures shall be conducted as requested by the Superintendent, ISO or designee. An internal audit of District network security will be conducted annually by District Technology staff. The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Electronic Access Security Controls

District staff 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. All staff are required to read and acknowledge applicable District policies via the Faculty Handbook sign-off form annually.

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

- **Identification/Authentication:** Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, confidential information, and/or internal information. Users will be held accountable for all actions performed on the system with their User ID. User accounts and passwords shall not be shared.
- **Authorization:** Access controls are maintained through a partnership between the technology department, human resources (HR) and data managers.

Additionally, only members of the District Technology staff will be granted access to domain level administrator and local machine administrator accounts in order to complete their job functions.

Access security is audited annually or whenever access permission requirements are changed for a particular application/software or when an application/software is no longer necessary.

Staff Users

All new staff accounts are authorized through an HR hiring process. Role-based permissions and security groups are used to establish access to all systems. If a staff member requires additional access, a request must be made directly to the ISO with a clear justification for access.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy. All contractor/vendor access must be approved by HR and the ISO. All contractors doing business on District premises must also pass a background check unless other security measures are addressed in a vendor contract. 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.

Password Security

The District will enforce secure passwords for all systems within their control. When possible, the District will utilize Single Sign On (SSO) or LDAP/Active Directory Integration to maintain optimal account security controls.

Remote Access

Access into the District's network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the District's network VPN appliance; no other method of remote access shall be granted without explicit authorization from the ISO. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within the District's network.

In the event that VPN access is needed by a contractor/vendor, access must be approved by the ISO. All VPN accounts will be reviewed at least annually.

Securing Data at Rest and Transit

District data security applies to all forms of data, including data stored on devices, data in transit and data stored on additional resources. Regular transmission of student data to internal and external services is managed by the technology department using a secure data transfer protocol.

Users must ensure that they are securely storing their data.

Usage and Dissemination

A consistently high level of personal responsibility is expected of all users granted access to the District's technology resources. All District staff, volunteers, contractors and agents who are granted access to critical and confidential information are required to keep the information secure. 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. Users must follow all guidelines outlined with Board policies.

Data Storage and Transmission

All staff and students that log into District owned computers will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data.

Cloud Storage and File Sharing

The term “Cloud Storage” is used to define all types of remote server storages accessed by users through the internet.

File Transmission Practices

Staff are responsible for securing sensitive data for transmission through email or other channels. Staff 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 services such as a single sign on provider is managed by the technology department using a secure data transfer protocol.

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the appropriate level of PCI compliance when handling such data.

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 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 downloaded, copied or printed indiscriminately or left unattended and open to compromise.

Oral Communications

Staff shall be aware of their surroundings when discussing PII and confidential information. This includes, but is not limited to, the use of cellular telephones in public areas. Staff shall

not discuss PII or Confidential Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or public areas.

Archival and Destruction

Once data is no longer needed, the ISO or designee will work with the data managers 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.

District Data Destruction Processes

The District will regularly review all existing data stored on District provided storage for the purposes of ensuring data identification and appropriate destruction. Data destruction processes will align with School Board Policy. District data managers will regularly review systems and data to ensure that data that is no longer needed is destroyed.

Asset Disposal

The District will maintain a process for physical asset disposal in accordance with School Board Policy. 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.

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. 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 District's Technology Disaster Recovery Plan outlines critical staff, responsibilities, and processes in the event of a disaster or critical data loss. The District shall maintain a list of all critical systems and data, including contact information. The Technology Disaster Recovery Plan shall include processes that enable the District to continue operations and efficiently restore any loss of data in the event of fire, vandalism, natural disaster, or critical system failure.

Data Breach Response

New Hampshire's data breach law (RSA 359-c:19, 20, 21) is triggered when a School District computer system is breached and personal information 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. 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 incidents. 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.

Appendix A - Definitions

Confidentiality: Data or information is not made available or disclosed to unauthorized persons.

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 staff.

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: Facts or information. Data can be in any form; oral, written, or electronic.

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 operational 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. The owner of information has the responsibility for:

- knowing the information for which she/he is responsible.
- determining a data retention period for the information according to Board policy and state statute.
- ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the data used or created.
- reporting promptly to the ISO the loss or misuse of data.
- initiating and/or implementing corrective actions when problems are identified.
- following existing approval processes for the selection, budgeting, purchase, and implementation of any digital resource.

Information Security Officer: The Information Security Officer (ISO) is responsible for working with the Superintendent, Data Governance Team, data managers, data owners,

and users to develop and implement prudent security policies, procedures, and controls. The ISO will oversee all security audits and will act as an advisor to:

- data owners for the purpose of identification and classification of technology and data related resources.
- systems development and application owners in the implementation of security controls for information on systems, from the point of system design through testing and production implementation.

Systems: Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV 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 acceptable-use policies.

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, State Assigned Student Identification, date and place of birth, mother‘s maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

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

User: The user is 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. Parental permission is required to gather certain information.

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.

IDEA: The Individuals with Disabilities in Education Act (IDEA) is a law that makes available a free appropriate public education to eligible children with disabilities throughout the nation and ensures special education and related services to those children.

PCI DSS: The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments.

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 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 RSA 189:68 Student Privacy

- NH RSA 189:68-a Student Online Personal Information

New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data

New Hampshire State RSA Chapter 359-C Right to Privacy:

• 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 to:

- ensure proper management, legality and security of information systems,
- increase data integration capability and efficiency,
- and minimize malicious code that can be inadvertently downloaded.

New Resource Acquisition

Staff are required to complete steps outlined under the staff section of the District's Student Technology Use and Data Privacy website. An online request form is required for any new digital resources that either has an associated cost or collects staff or student data. All staff must adhere to the following guidelines regarding digital resource acquisition:

- Contracts 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. Staff should speak with their building Technology Integrator before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.
- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets District business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the appropriate Assistant Superintendent, Curriculum Specialists and the Director of Technology, or designee, prior to purchase.

All new resources shall be properly evaluated against the following criteria, when applicable:

- Impact on technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
    - The District continues to own the data shared, and all data must be available to the District upon request.

- The vendor's access to and use of District data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the District. If metadata is collected, it will be protected to the same extent as the District's confidential or critical information.
- District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
- The provider will comply with District guidelines for data transfer or destruction when contractual agreement is terminated.
- No API will be implemented without full consent of the District.
- All data will be treated in accordance to federal, state and local regulations
- The provider assumes liability and provides appropriate notification in the event of a data breach.

Note: Exceptions can be made by the ISO when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent permission is requested from parents during the yearly online registration process for District vetted and approved applications and tools.

Approved Digital Resources

In order to ensure that all digital resources used meet security guidelines and to prevent software containing malware, viruses, or other security risk, digital resources that have been vetted are categorized as Approved or Denied.

- A list of vetted software will be maintained on the District Technology Use and Student Data Privacy website.
- It is the responsibility of staff to submit a request to use a new digital resource if a resource is not listed.
- Digital resources that are denied or have not yet been vetted will not be allowed on District owned devices or used as part of District business or instructional practices.

Digital Resource Licensing/Use

All computer software licensed or purchased for District use is the property of the District and shall not be copied for use at home or any other location, unless otherwise specified by the license agreement.

All staff must adhere to the following guidelines regarding digital resource licensing/use:

- Only approved District resources are to be used.
- District software licenses will be:
  - kept on file in the technology office.
  - accurate, up to date, and adequate.
  - in compliance with all copyright laws and regulations.

    - in compliance with District, state and federal guidelines for data security.
- Software installed on District systems and other electronic devices will have a current license on file or will be removed from the system or device.
- Resources with or without physical media (e.g. downloaded from the Internet, apps, or online) shall still be properly vetted and licensed, if necessary, and is applicable to this procedure.
- Under no circumstances can staff act as a parental agent when creating student accounts for online resources; resources requiring this permission must be approved at District level.

Appendix D - Data Security Checklist

A thorough risk analysis of all District data networks, systems, policies, and procedures shall be conducted as requested by the Superintendent, ISO or designee. An internal audit of District network security will be conducted annually by District Technology staff.

The Data Security Checklists examine the types of threat that may affect the ability to manage and protect the information resource. The analysis also documents any existing vulnerabilities found within each entity, which could potentially expose the information resource to threats. Finally, the analysis includes an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information is determined. The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Data Security Checklist for District Hosted Systems

- Inventory and classification of data on systems
- Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)
- Physical security of system
- Location within network including network systems protection (firewall, content filter) and if system is externally facing or only allows for District network access
- Access controls including password security (can District password requirements be enforced)
- Authentication methods (LDAP/Active Directory, Single Sign On, District managed account, user managed account)

Data Security Checklist for Provider Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)
- Contract, terms of service and privacy policy are current and meet District data security requirements
- Provider has adequate data security measures including data management and incident response
- Authentication methods (LDAP/Active Directory, Single Sign On, District managed account, user managed account)

Appendix E - Data Classification Levels

Personally Identifiable Information (PII)

PII is information about an individual maintained by an agency, including:

- Any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Unauthorized or improper disclosure, modification, or destruction of this information could violate state and federal laws, result in civil and criminal penalties, and cause serious legal implications.

Confidential Information

Confidential Information is very important and highly sensitive material that is not classified as PII. This information is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access. Examples of confidential information may include: student records, personnel information, key financial information, proprietary information, system access passwords and encryption keys.

Unauthorized disclosure of this information to individuals without a business need for access may violate laws and regulations, or may cause significant consequences for the District, its staff, parents, students or other stakeholders. Decisions about the provision of access to this information shall always be cleared through the data manager and/or ISO.

Internal Information

Internal Information is intended for unrestricted use within the District and in some cases within affiliated stakeholders. This type of information is already widely-distributed within the District, or it could be distributed within the organization without advance permission from the information owner. Examples of Internal Information include internal policies and procedures and handbooks.

Unauthorized disclosure of this information to outsiders may not be appropriate due to copyright, legal or contractual provisions.

Directory Information

Directory Information is information contained in an education record of a student that generally would not be considered harmful or an invasion of privacy if disclosed without the

consent of a parent or eligible student. The school District designates the following items as directory information:

- Student's name
- Address
- Telephone listing
- Electronic mail address
- Photograph
- Date and place of birth
- Major field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received
- The most recent educational agency or institution attended
- Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user
- A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.

Public Information

Public Information has been specifically approved for public release by the Superintendent or appropriate District administrator. Examples of public information may include patron mailings and materials posted to the District's website.

This information may be disclosed outside of the District.

Appendix F - Securing Data at Rest and Transit

All staff and students that log into a District owned computer will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on the local device. It is important to note that this data is not a part of the District's continuity plan, and thus will not be backed up by the District's backup solution.

Confidential and critical information will be saved and maintained in a secure manner using encryption or other password-protected security measures. Likewise, when data is transmitted, the District will use encryption or password-protected security measures.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. Users are responsible for all digital content on their District provided cloud storage. The term "File Sharing" is used to define all activities that share access to digital information whether in the cloud or on District administered mapped drives.

External Storage Devices

The term "External Storage Devices" is used to define all portable storage devices used by staff and students. While the District recognizes the advantages for staff and students to maintain information on these devices, users are strongly encouraged to rely on their District provided account for all storage needs.

File Transmission Practices

- Staff are responsible for securing sensitive data for transmission through email or other channels. When possible, staff should de-identify or redact any PII or confidential information prior to transmission.
- Staff should never include a password in any electronic communication unless directed to do so by Technology Staff.
- Staff should not transmit files labeled classified, confidential, or restricted through email or third party file transfer services without District approval.
- Regular transmission of student data to services such the District Library Management system, Food Service Management system and Single Sign On Provider system is managed by the technology department using a secure data transfer protocol. All such services are approved by the Director of Technology.

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the following requirements and appropriate level of PCI compliance when handling such data:

- Never store cardholder data on District systems or in written form. 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 the approved system.
- Never request cardholder information to be transmitted via email or any other electronic communication system.
- Payment information shall be entered directly into the approved payment system by individuals 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 the payment system.

Appendix G - Physical Security Controls

The following physical security controls shall be adhered to:

- Network systems shall be installed in an access-controlled area. The area in and around the computer facility shall afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
- Monitor and maintain data centers' temperature and humidity levels.
- File servers and/or storage containing PII, Confidential and/or Internal Information shall be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
- Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss.
- Computers and other systems shall be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
- Monitor and control the delivery and removal of all data-storing technological equipment or systems. Maintain a record of all such items entering or exiting their assigned location using the District approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology department.
- Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.

Appendix H - Asset Management

Data security must be maintained through the life of an asset, including the destruction of data and disposal of assets. Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as a system, asset or device.

All involved systems and information are assets of the District and are expected to be protected from misuse, unauthorized manipulation, and destruction.

Inventory

All technology devices or systems considered an asset are inventoried by the technology department. This includes, but is not limited to, network appliances, servers, computers, laptops, and mobile devices. The technology department will conduct annual inventory verification of all District devices. It is the responsibility of the technology department to update the inventory system to reflect any in-school transfers, in-District transfers, or other location changes for District technology assets.

Disposal Guidelines

Assets shall be considered for disposal in accordance with state/federal regulations and School Board Policy. The following considerations are used when assessing an asset for disposal:

- End of useful life
- Lack of continued need
- Obsolescence
- Wear, damage, or deterioration
- Excessive cost of maintenance or repair
- Salable value

The Director of Technology shall approve disposals of any District technology asset.

Methods of Disposal

Once equipment has been designated and approved for disposal (does not have salable value), it shall be handled according to one of the following methods. It is the responsibility of the technology department to update the inventory system to reflect the disposal of the asset.

Appendix I - Virus, Malware, Spyware, Phishing and SPAM Protection

Virus, Malware, and Spyware Protection

District PC desktops, laptops, and file servers are protected using enterprise virus/malware/spyware software. Definitions are updated daily and an on-access scan is performed on all "read" files continuously. A full scheduled scan runs weekly. A full scheduled scan is performed on all servers weekly during non-peak hours. All files and systems are scanned.

Internet Filtering

Student learning using online content and social collaboration continues to increase. The District views Internet filtering as a way to balance safety with learning—letting good content, resources, and connections in while blocking the bad. To balance educational Internet resource and application use with student safety and network security, the Internet traffic from all devices on the District network is routed through the District firewall and content filter. Filtering levels are based on the role of the user, staff or student and student grade level. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing.

Security Patches

Server patch management is performed regularly. Security patches are applied on an as needed basis, but at least bi-weekly.

Appendix J - Account Management

Access controls are essential for data security and integrity. The District maintains a strict process for the creation and termination of District accounts. All new staff accounts are authorized through an HR hiring process prior to creation. Role-based permissions are used to establish access to all systems. Access security is audited at least annually or whenever access permission requirements are changed for a particular application/software or when an application/software is no longer necessary.

Staff Accounts

When a staff member is hired by the District, the following process ensures that each staff member has the correct access and permissions to the resources that are required for their position.

- Notification of a new staff member is sent from Human Resources to the Technology Department. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology Department creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s).
- Any exception to permissions must be approved by the Director of Technology.
- When a staff member's employment is ended, either by termination or resignation, account permissions are revoked in one of two ways.
    - In the event of termination, HR will notify the Technology Department via email or phone call requiring the account to be disabled at once, preventing any further access to District resources.
    - In the event of resignation, HR will notify the Technology Department via email indicating the termination date. The account is disabled at the end of business on the termination date, preventing further access to District resources.
    - In the event that a user having elevated permissions to any system separates from the District, additional measures are taken to ensure that all elevated accounts to those systems are secure.

Local/Domain Administrator Access

Only members of the District Technology staff will be granted access to domain level administrator and local machine administrator accounts in order to complete their job functions.

Remote Access

Access into the District's network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the District's network VPN appliance; no other method of remote access shall be granted without explicit authorization from the ISO. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protections as information stored and accessed within District's network.

In the event that VPN access is needed by a contractor/vendor, access must be approved by the ISO. The Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

All VPN accounts will be reviewed at least annually.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by HR and ISO. All contractors doing business on District premises must also pass a background check unless other security measures are addressed in a vendor contract. 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.

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

Staff are entered into the District's student information system. Only staff whose roles require access are provided accounts for the system. The following minimum information is entered for each staff member:

- Building/Site location
- Status - Active
- Staff Type
- District Email Address
- Primary Alert Phone Number and Cell phone number

Access accounts for the District's SIS are set up based on staff role/position, building and required access to student data and are assigned by the Director of Technology or designee. Teacher accounts are created for all staff responsible for taking student attendance and entering and maintaining grades. Teacher accounts login to the SIS

Teacher Portal. Staff assigned a Teacher account only have access to students they teach or provide services to. Administrative accounts are created based on the staff member's role/position and function and further restrictions to data are controlled through security groups. Security groups control access permissions to certain data sets such as attendance, demographic data, grades, discipline etc. and whether the staff member can view or maintain data. Additional page level permissions are assigned to the security groups.

Financial System

All staff members are entered into the District's financial system for the purpose of staff payroll and HR tracking. Staff access to their individual payroll information is granted through the employee portal. Only staff requiring access are provided accounts for the financial/personnel system.

After basic information and user ID are created, a security role is assigned to the account granting them access to designated areas of the financial system to complete their job responsibilities.

Special Education System

The State of New Hampshire provides the District access to the NH Special Education Information System (NHSEIS) that houses all student IEP information. Access to accounts NHSEIS is maintained by the District's Director of Special Education office through the

MyNHDOE single sign-on portal. A user role determines the user's authority and applicable permissions within the NHSEIS system.

Health Software System

School District Nurses, Nurse Substitutes and Technology Staff are the only staff members granted access to the District's Health Software system. Technology Staff access is for the purpose of upgrades, and technical support for the use of the system. The medical data that is collected and maintained by the school nurses on the system includes immunizations, conditions, medications, and clinic logs (Time in/out of clinic and action taken). School nurses are the only accounts that can view and maintain medical information.

Food Services System

The District uses a Food Services software management system to track data and perform functions necessary for the efficient operations of the Food Service Program. Food service staff are granted accounts with access to only the parts of the system that are necessary to complete their job functions. Technology Staff access is for the purpose of upgrades, and technical support for the use of the system and cash registers. Strict security roles and permissions are in place to ensure that confidential information is only viewable by authorized staff.

Appendix L - Password Security

The District requires the use of strictly controlled passwords for network access and for access to secure sites and information. All passwords to District systems shall meet or exceed the below requirements.

- Passwords shall never be shared with another person.
- When possible, user created passwords should adhere to the same criteria as required for District network access.
- When creating a password for secure information or sites, it is important not to use passwords that are easily guessed due to their association with the user (i.e. children's names, pets' names, or birthdays).
- Users and staff who have reason to believe a password is lost or compromised must notify the Director of Technology or designee as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

District network access to resources managed through LDAP/SSO:

- Passwords must be "strong," and must be a minimum of 8 characters long.
- Your password must not be too similar to your username.
- Do not use your District password for any non-District systems.
- Where possible, system software should enforce the following password standards:
    - Passwords routed over a network shall be encrypted.
    - Passwords shall be entered in a non-display field.
    - System software shall enforce the changing of passwords and the minimum length.
    - System software shall disable the user password when more than five consecutive invalid passwords are given.

Appendix M - Technology Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable the District to respond effectively and efficiently to a natural disaster or critical failure of the District's data center and/or core systems. The objectives during a natural disaster or critical failure are the following:

- Minimize the loss or downtime of core systems and access to business critical data.
- Recover and restore the District's critical systems and data.
- Maintain essential technology resources critical to the day to day operations of the District.
- Minimize the impact to the staff and students during or after a critical failure.

Planning Assumptions

The following planning assumptions were used in the development of the TDRP:

- There may be natural disasters that will have a greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a disaster.
- There is the possibility of complete loss of the current data center.
- We will have adequate storage to recover systems.
- District data is housed at the District data center and backed up in the cloud.
- District data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

The District has appointed the following people to the disaster recovery/critical failure team: Director of Technology, Network Administrator, Technology Services Assistant, Data Management Specialist, and Technology Support Technician.

In the event the TDRP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determining the impact of the natural disaster/critical failure.
- Communication of impact and or loss, and updates of progress to the Superintendent.
- Communication of outages and updates to District staff.
- Oversight of the TDRP implementation and restoration of critical systems and data.
- Allocation and management of technology staff during the event.

- Working with manufacturers and/or vendors during the recovery and restoration of critical systems and data.
- Oversight of TDRP implementation debrief.

Activation

The TDRP will be activated in the event of the following:

- A natural disaster has occurred and affects the operation of the District's data center. A natural disaster includes but is not limited to the following: tornado, earthquake, lightning, and flood.
- A fire has impacted the data center.
- Water or flooding has impacted the data center.
- Critical system failure.

The Information Security Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent's Leadership Team will assume the role of IRM, with assistance from the IRT.

Notification

The following groups will be notified in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- District Staff
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication is available at the time. This could include any one or combination of the following:

- Phone
- Email
- Social Media/Website
- Radio or Television

The TDRP team will work with the Superintendent on which information will be conveyed to each above group and what means will be used.

Implementation

The TDRP team has the following in place to bring the District back online in the least of amount of time possible:

- Maintained spreadsheet listing all server names , physical and virtual, and their function. A hard copy of this document will be secured at the technology office.
- Maintained a secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.
- The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and the cloud.
- In the event of a critical system failure, the District can restore that server back to our current environment from the backup solution.

Deactivation

The TDRP team will deactivate the plan once services are fully restored.

Evaluation

An internal evaluation of the TDRP response will be conducted. This will entail gathering documentation from the response and feedback from all stakeholders and incorporate into an after action report and corrective action plan. The result will be an update to the TDRP and other emergency response plans as appropriate.

Appendix N - Data Breach Response Plan

Objectives

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

- Convene the Incident Response Team (IRT) as necessary.
- Validate and contain the data security breach.
- Analyze the breach to determine scope and composition.
- Minimize impact to the staff and students after a data breach has occurred.
- Notification of data owners, legal counsel, state/federal agencies and law enforcement as deemed necessary.

Planning Assumptions

The following planning assumptions were used in the development of TDBP:

- There may be data breaches that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a data breach.
- District data is backed up.
- Some District data is hosted by 3rd party providers.

Data Breach/Incident Response Team

The District has appointed the following people to the data breach/incident response team: Director of Technology, Network Administrator, Technology Services Assistant, Data Management Specialist, and Technology Support Technician.

In the event the TDBP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determine the nature of the data compromised and its impact to staff, students and the District itself.
- 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 and Business Administrator.
- Coordinate with the Superintendent to ensure communication with District staff and or parents as deemed appropriate.
- Oversight of the TDBP implementation and data breach resolution.
- Allocate and manage technology 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.
- Oversight of TDBP implementation debrief.

Activation

The TDBP will be activated in the event of the following:

- A data breach has occurred and affects the District itself. A data breach includes but is not limited to an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
- Personal Health Information (PHI) has been compromised.
- Personally Identifiable Information (PII) has been compromised.
- Confidential or sensitive data has been compromised.
- Network hack/intrusion has occurred.

The Information Security Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent's Leadership Team will assume the role of IRM, with assistance from the IRT. The breach response and reporting process will be documented according to state and federal requirements. The Director of Technology will work with the Superintendent to dispense and coordinate the notification and public message of the breach.

Notification

The following groups will be notified in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- District Staff
- Parents and Students
- Vendors

Information will be disseminated to the above groups through whichever means of communication deemed appropriate. This could include any one or combination of the following:

- Email
- Social Media/Website
- Radio or Television
- Written Notice
- Phone

The TDBP team will work with District leadership on which information will be conveyed to each above group, timing of that communication and what means will be used.

Implementation

The TDBP team has the following processes in place to contain the data breach in the least of amount of time possible:

- Data inventory of all systems containing sensitive data. A hard copy of this document will be secured at the technology office.
- Data dictionary of all District hosted information systems. A hard copy of this document will be secured at the technology office. Due to non- disclosure agreements, this data may not be available in other locations/formats. The appropriate vendor(s) can be contacted for this information.
- Maintained spreadsheet listing all server names, physical and virtual, and their function. A hard copy of this document will be secured at the technology office.
- Maintained a secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.
- The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and offsite.

The following will take place during the incident response:

- The members of the IRT will be assembled once a breach has been validated. The IRT will be composed of the Director of Technology, Network System Administrator, and Information Technology Systems Specialist. Additional members of the District's administrative team and technology department may be designated to assist on the IRT.
- The IRT will determine the status of the breach, on-going, active, or post-breach. For an active and ongoing breach, the IRT will initiate appropriate measures to prevent further data loss. These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.
- The IRT will work with the data managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
- The IRM will work with legal counsel and the Superintendent's Leadership Team to determine appropriate course of action pursuant to state statute. This includes notification of the authorities, and local law enforcement.
- Collaboration between the authorities and the IRT will take place with the IRM. The IRT will work with the proper authorities to make sure any and all evidence is properly handled and preserved.

- On advice from legal counsel, an outside party may be hired to conduct the forensic investigation of the breach. When the investigation has concluded, all evidence will be safely stored, recorded or destroyed (where appropriate).
- All affected data, machines and devices will be identified and removed from the network as deemed appropriate for the investigation. Interviews will be conducted with key personnel and facts of the incident will be documented and the evidence preserved for later examination.
- The IRT will work with the Superintendent's office to outline the notification of the data owners and those affected. Communication will be sent out as directed by legal counsel and advised by the District communications team. The types of communication will include, but not limited to, email, text message, postal mail, substitute notice and/or phone call.
- The IRM, in conjunction with the IRT, legal counsel and the Superintendent's Leadership Team will determine if notification of affected individuals is necessary. Once the determination is made to notify affected individuals, a letter will be written in accordance with all federal and state statutes, and local procedures. If it is determined that identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and filed at the Superintendent's office.

Deactivation

The TDBP team will deactivate the plan once the data breach has been fully contained.

Evaluation

Once the breach has been mitigated an internal evaluation of the TDBP response will be conducted. The IRT, in conjunction with the IRM and others that were involved, will review the breach and all mitigation steps to determine the probable cause(s) and minimize the risk of a future occurrence. Feedback from the responders and affected entities may result in an update to the TDBP and other emergency response plans as appropriate. Information security training programs will be modified to include countermeasures to mitigate and remediate previous breaches so that past breaches do not recur. The reports and incident review will be filed with all evidence of the breach.

Appendix O - Supporting Documents

SAU #6 Approved Software

https://drive.google.com/file/d/1H2iDE1BRerXLk2cQy7t2yFEtaA7fXY6D/view?usp=sharing