Data Governance Manual

2021

Approved by the Candia School Board

6-3-2021

SAU15

Henry W. Moore School

12 Deerfield Road

Candia, NH

03034

Table of Contents

1.0 - INTRODUCTION

The Candia School District are committed to protecting student and staff information through strong privacy and security methods. The privacy and security of this information is a significant responsibility, and we value the trust of our students, parents, and staff.

The Candia School District's Data Governance Manual includes information regarding the data governance team, data and information governance, applicable School Board policies, District 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. Definitions of terminology can be found in Appendix A: Definitions.

1.1 - Purpose

The School Board recognizes the value and importance of a wide range of technologies for a well rounded education by enhancing the educational opportunities and achievement of students. The Candia School District provide faculty and staff access to technology devices, software systems, network and Internet services to support research and education. All technology components must be used in ways that are legal, respectful of the rights of others, protective of juveniles, and that promote the educational objectives of the Candia School District.

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.

It is the policy of the Candia School District 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 staff and authorized district contractors or agents using confidential information will strictly observe protections put into place by the District.

1.2 - Scope

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

- Speech, spoken face to face, or communicated by telephone or any current and future technologies.
- Hard copy data either 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, or 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, Audio/Video 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 Candia School District and shall be protected from misuse, unauthorized manipulation and/or destruction.

1.3 - Data Governance Team

The Candia School District's Data Governance team consists of the following positions: Superintendent, Assistant Superintendent, Business Administrator, Human Resources Manager, and the individual district's Principal, Facilities Director, Director of Student Services, Food Service Director, 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). 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.

1.4 - 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). The Candia School District comply with the NH Minimum Standards for Privacy and Security of Student and Employee Data established in February, 2019. The Candia School District comply 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)
- Individuals with Disabilities in Education Act (IDEA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Pupil Rights Amendment (PPRA)
- 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 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 - 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

1.5 - Data User Compliance

The Data Governance Manual applies to all users of Candia School District's information including: staff, students, volunteers, and authorized district contractors or agents. All data users are to maintain compliance with Candia District School Board Policies and administrative procedures EHAB (Data Governance and Security), GBEF (Employee Use of District-Issued Computers, Devices and the Internet, formerly GCSA), GBEF-R (Employee Computer/Device and Internet Responsible Use Rules, formerly GCSA-R), JICL (Student Use of Computers, Devices and the Internet, formerly EGA), JICL-R (Student Technology Responsible Use, formerly EGA-R) and all policies, procedures, and resources as outlined within this Data Governance Manual 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 (mis)use of the district's technology resources.

Unless permission has been granted by the ISO or designee, no staff, vendor or other person may remove confidential or critical data from the district's premises, 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.

Staff 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 will end business relationships with any contractor who fails to follow the law, district policies or procedures, or the confidentiality provisions of any contract. In addition, the district reserves the right to seek all other legal remedies, including criminal and civil, and revocation of a staff member's educational certificate.

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

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

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

- Unauthorized disclosure of PII or Confidential Information.
- Sharing user accounts / IDs or passwords with others (with an exception for authorized technology staff for the purpose of support).
- Applying for a user account /ID under false pretenses.

- Using another person's account / ID or password.
- Unauthorized use of an authorized password to invade student or staff privacy by examining records or information for which there has been no request for review.
- The unauthorized copying of system or data files.
- Attempting to secure a higher level of privilege without authorization.
- Installation or use of unlicensed software or software not approved for district technology.
- The intentional, unauthorized altering, destruction, or disposal of district information, data and/or systems. This includes the unauthorized removal of technology such as but not limited to: laptops, internal or external storage, computers, servers, backups or other media, that may contain PII or confidential information.
- The introduction of computer viruses, hacking tools or other disruptive, harmful or destructive programs.

2.0 - SECURITY AND DATA GOVERNANCE PLAN

2.1 - Security and Risk Management

2.1.1 - Data Classification

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 (CI)

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 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 (II)

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
- 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.

This information may only be disclosed as permitted in School Board Policy JRA and JRA-R.

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.

2.1.2 - Risk Management

A thorough risk analysis of all the district's data networks, systems, policies, and procedures shall be conducted on a regular basis or as requested by the Superintendent or Director of Technology. The risk assessment shall be used as a basis for a plan to mitigate identified threats and risk to an acceptable level.

The Director of Technology administers periodic risk assessments to identify, quantify, and prioritize risks. Based on the periodic assessment, measures are implemented to mitigate the threats by reducing the amount and scope of the vulnerabilities.

Because technology security planning is primarily a risk management issue, this document and its associated standards and guidelines focus on the creation of a shared and trusted environment, with particular attention to:

- Common approaches to end-user authentication

- Consistent and adequate network, server and data management
- Appropriate uses of secure network connections
- Closing unauthorized pathways into the network

The district's use of the Internet for conducting official business has generated the following security concerns:

- Information Integrity - Unauthorized deletion, modification or disclosure of information.
- Misuse - The use of information assets for other than authorized purposes by either internal or external users.
- Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users.
- Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs.
- Computer Viruses - Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files, or devices on a system or through multiple systems in a network that may result in the destruction of data or the erosion of system performance.
- Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss of embarrassment to the organization.
- Component Failure - Failure due to design flaw or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component.
- Unauthorized additions and/or changes to infrastructure components.

To address these concerns, the district will take steps necessary to:

- Ensure secure interactions between and among business partners, external parties, and school District to utilize a common authentication process, security architecture and point of entry.
- Prevent misuse of, damage to, or loss of district hardware and software resources.
- Prevent unauthorized use or reproduction of copyrighted material by public entities.
- Ensure secure interactions between the district and outside agencies and ensure that there is a shared and trusted environment.
- Operate in a manner consistent with this Data Governance Manual and Board policies and procedures.
- Develop, implement, maintain and test security processes, procedures, and practices to protect and safeguard voice, video, and data computing and telecommunications facilities (including telephones, hardware, software and personnel) against security breaches.
- Train staff to follow security procedures and standards.
- Apply appropriate security measures when utilizing transactional internet-based applications.
- Ensure and oversee compliance with this policy.

2.1.3 - Maintenance of Policies, Standards, Guidelines, and Recommendations

Technological advances and changes in the business requirements of the district will necessitate periodic revisions to policies, regulations, procedures, guides and handbooks. The district is responsible for routine maintenance of these to keep them current. Therefore, the Department of Technology leadership will review and update technology security policies, regulations, procedures, guides, and handbooks at least annually or following any significant change to its business, computing or telecommunications environment. Examples of these changes include modifications to physical facilities, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization or budget.

Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties.

If the district purchases technology services from another organization, the district and the service provider will work together to make certain the technology security plan for the service provider fits within the district's security policies. The district will obtain a copy of the service provider's data privacy and security plan to determine if it complies with district requirements.

2.1.4 - Related Policy and Procedure Documents

Board Policy and Technology Usage Agreement

This document and its related procedures are governed by Board Policy EHB and their associated regulations and forms. Response plans and process level procedures will adhere to the standards set by board policy. Anyone who uses district technology is required to sign and abide by the appropriate approved technology usage agreement.

Disaster Recovery Plan

Technology staff will maintain a technology disaster recovery plan delineating the district's procedures for recovery from an unforeseen disaster or emergency. This plan will contain process level procedures for recovering critical technology platforms, telecommunications infrastructure and ensuring data security. Controls shall ensure that the district can recover from any damage to critical systems, data, or information within a reasonable period of time. Each school, department, or individual will be required to report any instances immediately to the Department of Technology for response to a system emergency or other occurrence (e.g., fire, vandalism, system failure and natural disaster) that damages data or systems. The Disaster Recovery Plan shall include the following:

- A prioritized list of critical services, data and contacts.
- A process enabling the district to restore any loss of data in the event of fire, vandalism, natural disaster or system failure.

- A process enabling the district to continue to operate in the event of fire, vandalism, natural disaster or system failure.
- Procedures for periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary. (See section 3.2 Disaster Recovery Plan)

Data Breach Response Plan

Technology staff will maintain an incident response plan detailing the district's response and recovery to security events including physical intrusion of secured areas, electronic intrusions, deception and fraud, hacking incidents, or any other unplanned or unwanted security event posing a threat to district data and/or systems. (See section 3.3 Data Breach Response Plan)

2.2 - Asset Security

2.2.1 - Physical Records

While electronic information may be accessed from the internet, PII/CI/II can be accessed through printed or physical materials such as hardcopy reports and external storage media.

Physical records on paper or electronic removable storage shall follow these guidelines for security:

- Records with PII/CI/II for long-term storage shall be stored in fireproof, locking file cabinets housed in a location with supervised access.
- File-cabinets shall be locked at all times other than when being accessed. Keys to file cabinets will not be accessible to unauthorized staff.
- Requests for records contained in the file cabinets shall be logged to indicate the requestor name, date, time and file(s) requested, and additional information as needed.
- Records with PII/CI/II removed from the file cabinets shall be stored in a locked private office, a locked desk drawer, a locked briefcase, or similar restricted access location.
- At no time should printed PII/CI/II material be left accessible and unsupervised, including after working hours.
- Retention times of physical records shall follow applicable board policies (EHB), and all applicable local, state and federal laws.
- Paper records may be digitized as appropriate. Storage of digital records is covered elsewhere in this document. Record retention shall follow EHB.
- PII/CI/II should not be printed/made into hardcopy except when necessary.
- Users who print PII/CI/II should use secure print to require the sender's physical presence at a shared or network printer to retrieve the hardcopy.
- Shredding of PII/CI/II paper records shall be accomplished only by staff who have authorization to see those records; shredding may be contracted to a service that can document the chain of custody and destruction.
- Records slated for upcoming destruction shall be kept secure until the time of their destruction.

- External storage devices with PII/CI/II to be destroyed shall be wipe and overwrite the data so that it is unrecoverable, or physically destroy the media.

2.2.2 - Software Standards and Procedures

The district shall abide by the following standards and procedures regarding all software that it owns or licenses:

- Software owned or licensed by the district may not be copied to alternate media (such as removable storage), distributed by email, transmitted electronically, or used in its original form on any device other than district resources without express permission from the Department of Technology.
- Software licensed to the district is to be used for its intended purpose according to the license agreement. Employees are responsible for using software in a manner consistent with the licensing agreements of the manufacturer. In no case is the license agreement or copyright to be violated. License agreements are maintained by the Department of Technology.
- All software installed on district computers must be owned or licensed by the district.
- All software purchased by the district must be installed on district-owned equipment, and may not be taken off-site without permission from the Department of Technology.
- No district owned software may be installed on a computer not owned by the district unless the license agreement specifically allows it and the installation is overseen by technology staff.

2.2.3 - Hardware Standards and Procedures

The district shall abide by the following standards and procedures regarding all hardware that it owns or leases:

- All workstations, printers, add-in cards, memory modules, and other associated equipment are the property of the district and should not be used for purposes other than those relevant to the execution of duties or sanctioned educational activities.
- No changes, modifications, additions, or equipment removals may be done without written notification to and approval from the Department of Technology.
- No information systems equipment should be removed from the district, with the exception of documented approval from the Director of Technology or his/her designee, for equipment to be used for off-site by a named, specific staff member.
- A standard platform is established for district computers and equipment by the Department of Technology Leadership Team and documented by the Manager of Technology Support Services.
- In order for effective software and network functioning, the district will make every effort to provide up-to-date and reliable hardware, including computers, servers, routers, switches, etc.

2.2.3.1 - Inventory

- Unless otherwise authorized by a member of the Department of Technology, all computer and network electronics connected to the district network must be owned/leased by the district and must be on the fixed asset inventory.
- The fixed asset inventory of all end-user devices will be maintained by the Department of Technology and will include the Device Name, Serial Number, Asset Tag Number, Location and Purpose that each device is being used for.
- The fixed asset inventory will be maintained in a database and updated as needed.
- A full walk-through inventory inspection will be conducted by the Department of Technology at least once a year.

2.2.3.2 - Hardware

- Non-standard hardware is only to be used if standard hardware is unavailable and only if approved by the Department of Technology Leadership Team.
- All hardware purchased by the district must be installed on district-owned equipment.

2.2.4 - Mobile Devices

A mobile device is defined as any handheld network capable computing device such as a smartphone or tablet. The district has established procedures which allow it to keep track of mobile devices used to access district information and the personnel who use them.

The Department of Technology will adhere to the following concerning mobile devices given to district personnel:

- If the device supports a passcode feature, the passcode lock shall be enabled at all times and entered by the user for access. The passcode lock shall be active when the device is idle.
- The loss or theft of a device must be reported to both the Department of Technology and the user's immediate supervisor as soon as the loss or theft is identified.
- Devices which have been configured to access district information or electronic mail shall have the capability to be remotely erased and rendered unusable.
- The Department of Technology will maintain a record of all assigned devices using the Mobile Device Inventory.

2.2.5 - Practices for Network Use

In accordance with Board Policy EHB, authorized employees may use the district's technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policies or procedures, hinder the use of the district's technology resources for the benefit of its students or waste district resources.

2.3 - Security Operations

2.3.1 - Data Transfer/Exchange/Printing

For Windows and Mac users: 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. Access to these files is restricted to the folder's owner (staff or student who is assigned) and district enterprise administrator accounts. Users should store all their files in their GSuite accounts.

For Chromebooks: Chromebook users are to store their data within their GSuite for Education Drive account.

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.

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 a district/building administrator and the Director of Technology.

2.3.1.1 - Electronic 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 accordance with this manual and all related board policies and procedures, and must be approved by the Department of Technology Leadership Team. All mass downloads of information shall include only the minimum amount of information necessary to fulfill the request.

2.3.1.2 - Visual Security and Printing

PII, Confidential Information, and Internal Information shall be stored in a manner inaccessible to unauthorized individuals. PII and Confidential Information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise. PII that is downloaded for educational purposes where possible shall be de-identified before use.

2.3.1.3 - 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 approved system.
- The district will never maintain a data system for payment information. All payment information will be stored and processed by a third party accessible through a secure portal.
- 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 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.

2.3.1.4 - 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. All staff and students are provided with a GSuite for Education account that provides unlimited storage. Users are responsible for all digital content on their district provided GSuite for Education Drive. When using cloud storage, staff and students must adhere to the following guidelines:

- Staff and students may not access cloud storage through third party applications outside of approved internet browsers and Google Drive App on Android & iOS. This will ensure that native operating systems do not replace cloud sharing security.
- Users need to be aware of default sharing settings on folders when they upload files. Users are required to limit sharing files to an as needed basis.
- Staff and students must ensure that any cloud storage providers used are approved by the district and meet district student data and data security standards.

- When exiting the district, students should responsibly copy their content to their own personal storage solution.
- When exiting the district, staff should ensure that they are only copying personal content that they created. Staff are prohibited from copying content that contains confidential information, student records or data.
- Data with personally identifiable information of staff or students may be posted to users' district provided Google Drive with appropriate security settings. Users may not post this data to other cloud sharing platforms without consent of district administration.
- Staff should never post any documents labeled classified, confidential, or restricted to any cloud storage including district provided Google Drive accounts without district approval.
- All users shall immediately report any cloud storage security problems of the district's technology resources to a teacher or administrator.
- Attempting to gain or gaining unauthorized access to cloud storage or the files of another is prohibited.
- As with other forms of district technology, district staff, students, and other GSuite for Education drive users have no expectation of privacy on data stored on this platform.
- 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. When file sharing, staff must adhere to the following guidelines:
- Users must abide by all policies and procedures regarding professional conduct and communication when sharing, reviewing, updating, commenting and re-sharing.
- When sharing content, users must ensure that other users accessing the information in the files have appropriate access to the information based on job function.
- All users shall immediately report any inappropriate sharing of the district's technology resources to an administrator.

2.3.1.5 - External Storage Devices

The term "External Storage Devices" is used to define all portable storage devices (including USB drives, rewritable CD/DVD, memory cards, and external hard drives) 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 GSuite for Education Drive account for all storage needs. When using external storage devices, staff must adhere to the following guidelines:

- Users are responsible for all content on external storage devices that have been connected to district technology resources.
- Users must ensure that they will not introduce harmful software including computer viruses, malware, non-district approved software, or hacking tools to district technology resources.
- Users must ensure that the data will remain secure through appropriate encryption or password protection when transferring files containing PII or protected information to an external storage device. Users should only keep the information stored on the external device for the duration of the project, and then promptly remove it.

- Staff should never transfer any documents labeled classified, confidential, or restricted to any external storage device.
- Staff should never transfer or create confidential data or student records on personal storage devices.

2.3.1.6 - Oral Communications

The district's 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. District 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 on public transportation.

2.3.1.7 - Audit Controls

Hardware, software, services and/or procedural mechanisms that record and examine activity in information systems that contain or use PII are reviewed by the Department of Technology staff annually. Department of Technology staff also regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.

2.3.1.8 - Evaluation

The district requires that periodic technical and non-technical evaluations of access controls, storage, and other systems be performed in response to environmental or operational changes affecting the security of electronic PII to ensure its continued protection.

2.3.2 - Security Incident Reporting

A security incident is defined as any event posing a threat to district data or systems. All security violations or suspected violations must be reported to the Department of Technology. The Department of Technology may take any measures deemed appropriate for the specific security violation as outlined in the Incident Response Plan. The Department will also work with the appropriate administrative party to ensure evidence is preserved and reported correctly, and contact the appropriate law enforcement if deemed necessary by the Incident Response Team. It is the responsibility of all district staff and any persons who utilize district technology to report suspected security violations as quickly as possible. Security breaches may be categorized as those pertaining to physical intrusions; electronic intrusions that include networks, servers and workstations; incidents related to catastrophic disasters; and breaches as a result of deception and/or fraud. Regardless of the category of incident, the district's focus is the protection of district assets, containment of damage and the restoration of service.

2.3.3 - Security and Data Logs

The Department of Technology archives specific log file types for a pre-defined duration. Documentation around specifically which logs are kept and what information they contain is documented in this manual under Network Security Administration Procedures.

2.4 - Communication and Network Security

2.4.1 - Firewall Requirements: Use, Functionality and Port Restriction

The district will maintain firewalls that provide borders of protection between the internal network and the connection to the Internet. Below are examples of what will not be permitted:

- No File Transfer Protocol (FTP) access is allowed from the Internet to a device on the district network.
- The district will not restrict FTP out of the network to a device on the internet provided the session / transfer is initiated from the network.
- No Local Area Network (LAN) protocols will be mapped to and/or from devices on the Internet (e.g. NetBios, NetBeui, NFS)
- No outbound port that has the potential of propagating industry-known malware will be allowed.

2.4.2 - Web Server: Connectivity and Security

The district maintains and houses web servers that reside on the district network and are accessible from the Internet. The district is required to “harden” the server by making sure that all the current operating system patches are applied and kept up to date, and by removing any unnecessary server processes. Web servers shall not be accessible directly from the Internet and should only be accessible through a firewall and/or load balancer.

2.4.3 - Email Functionality, Security, and Limitations

Email is filtered for viruses, phishing, spam, and spoofing using Google services.

- No Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) from Internet to mail servers inside the network will be allowed. The district will utilize a web interface Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure (HTTP/ HTTPS) to access email.
- No POP or IMAP from the network to private email accounts on the internet. The district will utilize and web interface (HTTP/HTTPS port) to access this email.
- Users will be instructed to never open any email attachments on the network except via district email through a web browser. Users will be instructed to use extreme caution when downloading and/or opening email attachments to ensure that the attachment is safe.
- Virus scanning is used on the district email system and on all attachments.

2.4.4 - Non-Educational/District-Business Related Network Traffic

Bandwidth has a high cost associated with its usage. The district network is implemented and maintained to allow district users to utilize automated systems and tools to facilitate their responsibilities and duties and meet their needs. The district network infrastructure must not be utilized for personal gain and/or entertainment.

2.4.5 - Wireless Access and Network Connectivity

The district will enable and configure encryption on all wireless traffic.

No installations of wireless devices, such as wireless access points, wireless printers, or wireless network cards, may be installed in the district by any person except technology staff. Proper configurations must be performed in order to protect the network.

Consideration for network connections will be based on the need for the connection as well as ensuring security and integrity of the network. Network access may be denied at the discretion of a member of the Technology Department with appeal to the Data Governance Team.

Changes to wired network connections are only to be performed under the direction of a member of the technology staff.

2.4.6 - Internet Filtering

Student learning using online content and social collaboration continues to increase. The Candia School District view Internet filtering as a way to balance safety with learning—letting good content, resources, and connections in while blocking harmful material. 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.

2.4.7 - Malware Prevention, Detection and Removal

The district will:

- Maintain real-time antivirus / malware protection software on the network including all servers and workstations.
- Be diligent about updating malware definition files.
- Removing infected devices from the network until such a time that the device can be cleaned / removed / made harmless.
- Ensure copies of malware-detection and eradication tools are kept offline to prevent any malware from modifying the detection tools. Technology staff will actively scan / check for malware online but will also periodically use the offline, trusted tools to scan systems.

- Malware checking systems approved by the Technology Department are employed using a multilayered approach (firewalls, filters, gateways, servers, computers, etc.) that ensures all electronic files are appropriately scanned for malware on a regular basis. Users shall not turn off or disable the district's protection systems or install other systems.

2.4.8 - Network Security Administration Procedures

- Normal logging process must be enabled on all host and server systems.
- Alarm and alert function as well as logging of any firewalls and other network perimeter access control systems must be enabled.
- Audit logs from the perimeter access control systems should be reviewed on a regular basis.
- Audit logs for servers and hosts on the internal, protected network should be reviewed on a regular basis.
- Users must be trained to report any abnormalities in system performance to technology staff.
- Users must notify Technology Department of violations of the CIPA law. All users must abide by CIPA. Violations will be reported to the proper legal authorities.
- All incident reports received by the Technology Department must be reviewed for symptoms that might indicate intrusive activity. Suspicious symptoms must be reported to the Technology Department.
- Any user who witnesses or suspects a security incident of any kind must report it to the Technology Department immediately. All security incidents will be dealt with following the procedures described in the Technology Incident Response plan.

2.5 - Identity and Access Management

2.5.1 - Access Controls

Physical and electronic access to information system that contains Personally Identifiable Information (PII) Confidential Information (CI), Internal Information (II) and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures are instituted as approved by the Data Governance Team. In particular, the Data Governance Team will document roles and rights to the student information system (SIS) and other similar systems.

Mechanisms to control access to PII, CI, II and computing resources include but are not limited to the following methods:

2.5.2 - Authorization

Access shall be granted on a "need to know" basis and shall be authorized by the Superintendent, Assistant Superintendent, principal immediate supervisor or Director of Technology. Specifically, on a case by case basis, permissions may be added to individual users in the student information system, again

on a need-to-know basis, and only in order to fulfill specific job responsibilities with the approval of the Data Governance Team.

2.5.3 - Identification / Authentication

Unique user identification (user ID) and authentication are required for all systems that maintain or access PII, CI, and/or II. Users shall be held accountable for all actions performed on the system with their User ID. User accounts and passwords will not be shared.

2.5.4 - Data Integrity

The district provides safeguards so that PII, CI, and II is not altered or destroyed in an unauthorized manner. Core data is backed up using a disaster recovery plan. In addition, listed below are methods that are used for data integrity in various circumstances:

- Transaction audit
- Disk redundancy (RAID)
- ECC (error correcting code) memory
- Checksums (file integrity)
- Data encryption
- Data wipes

2.5.5 - Transmission Security

Technical security measures are in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. Integrity controls and encryption (such as Secure Socket Layers - SSL) are implemented where appropriate.

2.5.6 - 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 network.

In the event that VPN access is needed by a contractor/vendor, access must be approved by the ISO. The Department of Technology 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.

2.6 - User Accounts

District Staff user accounts are automatically assigned according to the individual user's job responsibilities. This includes levels of permission for each account. The Technology Department will review the HR job title regularly to ensure that the appropriate level(s) of permission and access is assigned.

District student accounts will provide access only to the local resources deemed necessary by the Technology Department. Student accounts will be prevented from accessing other district resources. (See Appendix D).

- If a support vendor requires temporary access to district technology resources, their access must be restricted to that which is necessary for their function, and must be immediately revoked upon completion of their support task.
- User accounts for staff no longer employed by the district will be disabled.
- Users must lock or log off when leaving their computer.

2.7 - Requests for Additional Access and/or Permissions

Users requesting additional access or permissions levels will submit a Help Desk request. The ticket will be escalated to the data governance team who will then consider whether the request should be granted, and if so determine:

- The needed duration of the escalated access or permission.
- If the needed access or permission is a requirement for a particular individual or if it should be assigned to the HR job titles.

2.8 - Passwords

Passwords are personal identification keys that allow access to various technology resources on the district's network. Passwords help ensure that only authorized individuals gain access to a computer system, network device, application, file, data, etc. Passwords also help to establish accountability for all transactions and changes made to those technology resources. The district has enacted strict password policies in securing our local network. The following guidelines are used when developing password policies, with the exception of students in kindergarten through second grade.

Password Creation Requirements

- Passwords must contain at least eight nonblank characters.
- Passwords should be changed annually and not more than every 30 days.
- New passwords must not be any of the previous two passwords.
- Passwords should be complex.

- Passwords should not contain the user ID.
- Passwords should not include any personal information about the user that can be easily guessed: user's name, spouse's name, children's name, birthdate, etc.
- Passwords should not contain any simple pattern of letters or numbers such as "qwerty" or "xyz123".
- Passwords should not be trivial, predictable or obvious.
- Passwords should be memorized and not displayed for others to view.

Protecting Passwords

- Passwords will be required on all user accounts.
- Passwords must be unique to the users.
- Passwords must not be disclosed to anyone except when there is an overriding operational necessity (e.g., support issue).
- Passwords must be changed if anyone other than the authorized user learns the password.
- Passwords must not be left in a location accessible to others or secured in a location for which protection is less than that required for information that the password protects.
- Users must avoid sending passwords in clear text over the network.
- Passwords must be changed at least every school year.
- All student and staff computers will be automatically locked within an hour of inactivity.
- Teachers and/or staff members must never allow another user (such as a student or substitute teacher) to use their computer while they are logged in to the network. Teachers and staff have more privileges than students, such as access to grade books, and students should never have access to those rights.
- Students may never use another student, teacher, or staff member's password nor may they use a computer that is already logged in as another user.
- If a user suspects their password has been cracked or stolen, they must inform the Department of Technology and change their password immediately.

2.9 - Physical Access: Security Guidelines and Recommendations

The district recognizes that a majority of security incidents, vandalism, and even accidental acts that lead to disruption of services can be attributed to deficiencies in physical security. The guidelines below were established in order to maintain adequate physical security for the district.

Responsibility

The Technology department is responsible for the physical security of district owned devices. This includes but is not limited to desktops, laptops, cell phones, hotspots, monitors, printers, projectors, televisions and SmartBoards.

The Technology department is responsible for the physical security of district network devices. This includes but is not limited to switches, routers, servers, racks, access points and security cameras.

Location

- Network and computer equipment will be located away from windows or any other place that allows easy access by unauthorized individuals.
- Network equipment and computer equipment will be located in places that can be environmentally controlled.

Access

- Rooms or closets that contain District Wide Area Network routers and servers must be locked at all times, including remote offices. Department of Technology staff are the only authorized party to enter these rooms.
- Wiring closets must be locked at all times. Department of Technology staff are the only authorized party to enter these closets.
- Switches are to be secured in a lock protected closet. Department of Technology staff are the only authorized party to enter these closets.
- A secure access system should be installed and maintained in the main datacenter(s). Only authorized personnel are allowed access to the datacenter(s) without an escort.
- No computer connected to the network should ever be left unattended by the user who logged in to the network. All users must log off the network and the computer at the end of the day.
- All classrooms, offices, meeting rooms, etc. that house computers must be locked and secured when the room is vacated.

PII, Confidential and Internal information Access

- Access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals. At a minimum, staff passwords shall be changed annually.
- No PII, Confidential and/or Internal Information shall be stored on a device itself such as a hard drive, mobile device of any kind, or external storage device that is not located within a secure area.
- No technological systems that may contain information as defined above shall be disposed of or moved without adhering to the appropriate School Board Policy DN - School Property Disposal Procedure
- It is the responsibility of the user to not leave these devices logged in, unattended and open to unauthorized use.

Environmental and Electrical Measures.

At a minimum, district data centers and telecommunications rooms should employ the following environmental controls:

- Fire protection in these areas shall comply with NFPA 75: Standard for the Fire Protection of Information Technology Equipment and NFPA 76: Standard for the Fire Protection of Telecommunications Facilities
- Electrical systems for critical computer equipment must include Uninterrupted Power Systems (UPS). Surge protectors should be considered for equipment sensitive to power fluctuations, at the discretion of the Technology Department.
- Adequate room temperature and humidity must be maintained to the specifications of the hardware vendor.

2.10 - Disposal

All devices that are leaving the service of the district shall be wiped of all data. Disposal guidelines are in Appendix C.

3.0 - 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.

3.1 - Business Continuity

The District's administrative procedure EHB, delineates the timeline for data retention for all district data. The District will maintain systems that provide local and off‑site data backup. These systems shall allow for the full recovery of critical systems in the event of a disaster. The district will test local and off‑site backups of critical systems quarterly.

3.2 - Disaster Recovery Plan

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.

3.2.1 - Objectives

The primary purpose of the Disaster Recovery Plan (DRP) is to enable the Candia School 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.

3.2.2 - Planning Assumptions

The following planning assumptions were used in the development of Candia's DRP:

- There may be natural disasters that will have 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 district data center and backed up off-site.
- District data is hosted by third party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

3.2.3 - Disaster Recovery/Critical Failure Team

Candia has appointed the following people to the Disaster Recovery Plan (DRP): Director of Technology, Superintendent and designated members of the Data Governance Team as applicable to the incident. When the DRP 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 DRP implementation and restoration of critical systems and data.
- Allocation and management of Candia staff during the event.
- Working with manufacturers and/or vendors during the recovery and restoration of critical systems and data.
- Oversight of DRP implementation debrief.

3.2.4 - Activation

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

- A natural disaster has occurred and affects the operation of the District’s data center / core systems. 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 Incident Response Team (IRT).

3.2.5 - Notification

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

3.2.6 - Implementation

The DRP team has the following in place to bring the District back online as expeditiously as 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. An electronic version will be housed on Google Drive.
- Maintained 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 off-site location.
- In the event of a critical system failure, the District can restore that server back to our current environment from the backup solution.

3.2.7 - Deactivation and Evaluation

The DRP team will deactivate the plan once services are fully restored. An internal evaluation of the Candia's DRP 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 DRP and other emergency response plans as appropriate.

3.3 - Data Breach Response Plan

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 (ie-FERPA), 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.

3.3.1 - Objectives

The purpose of the Data Breach Plan (DBRP) is to enable the Candia School 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 incident. The objectives of the DBRP 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.

3.3.2 - Planning Assumptions

The following planning assumptions were used in the development of Candia's DBRP:

- 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.

3.3.3 - Data Breach/Incident Response Team

Candia School District has appointed the following people to the data breach/incident response team (IRT): Director of Technology, Superintendent and designated members of the Data Governance Team as applicable to the incident.

In the event the DBRP 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 Superintendent to ensure communication with district staff and or parents as deemed appropriate.
- Oversight of the DBRP 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 DBRP implementation debrief.

3.3.4 - Activation

The DBRP 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.

3.3.5 - Notification

The following groups may 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 deemed appropriate. This could include any one or combination of the following:

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

The DBRP 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.

3.3.6 - Implementation

The DBRP 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. An electronic version will be housed on the Technology Departments Team Drive.
- 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. An electronic version will be housed on the Technology Departments Team Drive.
- Maintained 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 confirmed. Additional members of the Candia School 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 recurrences.
- 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.

3.3.7 - Deactivation and Evaluation

The DBRP team will deactivate the plan once the data breach has been fully contained. Once the breach has been mitigated an internal evaluation of the Candia's DBRP 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 DBRP 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.

4.0 - SERVICE PROVIDER DATA PROTECTION AND PRIVACY

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 the Superintendent or designee. 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.

4.1 - Student Data Privacy Consortium

Candia District are members of the SDPC and will utilize its contracts and resources with service providers.

The Student Data Privacy Consortium (SDPC) is a unique collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns. The Consortium also leverages work done by numerous partner organizations but focuses on issues being faced by "on-the-ground" practitioners.

Consortium Goals

- Establish a community of stakeholders who have various needs addressed through policy, technology and/or effective practice sharing around effective privacy management,
- Identify projects that have on-the-ground and real-world impact on student data privacy enabling schools, districts, state and vendors find resources, adapt them to their unique context and implement needed protections,
- Development of tools and resources to address operational issues not currently being addressed,
- Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work,
- Development of a clearinghouse of student data privacy operational issues and resources to support schools, districts, states and vendors in managing those issues – no matter where the resources originate.

5.0 - DIGITAL RESOURCE / SOFTWARE ACQUISITION AND USE

5.1 - 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.

5.2 - 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, School Board policy, and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

The Candia School District has an established process for vetting new digital resources. Staff are required to complete steps outlined within the District's Student Technology Use and Data Privacy portion of the website, to ensure that all new resources meet business and/or instructional needs as well as security requirements.

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 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.

A current list of all vetted and approved software systems, tools and applications will be published on the Candia School District's Technology Use and Student Data Privacy page on the ~~Candia School District's~~ SAU 15 website.

5.3 - 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. The form is available on the Candia School District's Technology Use and Student Data Privacy page on the SAU15 website
- 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.

5.4 - 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 Candia School 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 the district level.

5.5 - 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 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.

The District will audit data imports annually. These audits should include:

- Review of provider's terms of service to ensure they meet the District's data security requirements.
- Verification that software imports are accurate and pull the correct information.
- Verification that, when applicable, the staff, students and classes included in the imports are still necessary for instructional purposes (only those that need data collected are included in import).
- Determine if the fields included in the imports are still necessary for intended purpose.

5.6 - Software Inventory

~~Candia School District will update annually a list (available here when complete) of all digital resources that access PII. These include licensed software (e.g. Microsoft Windows 10), web browser extensions (e.g. Chrome Draftback or Screencastify), and websites requiring an account (e.g. Microsoft Office 365).~~

A current list of all vetted and approved software systems, tools and applications will be published on the Candia School District's Technology Use and Student Data Privacy page on the SAU 15 website.

Candia District are members of the NHCTO (NH Chief Technology Officer) chapter of CoSN (Consortium on School Networking). NHCTO is a partner in the Student Data Privacy Consortium (SDPC) (www.sdpc.a4l.org). The SDPC provides resources for members to use for software vetting including a database of products and vendors that meet state requirements for data privacy and security.

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. A user of data is expected to:

- access information only in support of their authorized job responsibilities.
- comply with all data security procedures and guidelines.
- keep personal authentication confidential (user IDs, passwords, secure cards, PINs, access codes).
- report promptly to the ISO the loss or misuse of data.
- follow corrective actions when problems are identified.

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.
https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

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.
https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy

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.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

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.
https://www.hhs.gov/hipaa/index.html

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.
https://sites.ed.gov/idea/

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.
www.pcisecuritystandards.org

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. https://www2.ed.gov/policy//gen/guid/fpco/ppra/index.html

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 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: Disposal Guidelines

Assets shall be considered for disposal in accordance with state/federal regulations and School Board Policy DN - School Properties Disposal Procedure. 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.

Discard

All technology assets shall be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. When possible, any re-usable hardware that can be used as parts to repair and/or maintain district technology assets shall be removed (motherboards, screens, adapters, memory). In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the school district.

A district-approved vendor shall be contracted for the disposal of all technological systems/equipment. The vendor shall provide written documentation verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data.

Under no circumstances should any technological systems/equipment be placed in the trash.

Donation/Gift

In the event that the district determines that an asset shall be donated or gifted, systems shall be wiped clean of Personally Identifiable Information (PII), Confidential, and/or Internal Information prior to leaving the school district. The Candia School District will not support or repair any equipment that is donated. In addition, software licenses are not transferred outside the district. Therefore, systems must be returned to factory installation prior to donation.

APPENDIX D: User Roles and Security

Student Information System (SIS)

Staff are entered into the Candia School 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 setup 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. PowerSchool administrative accounts log into the SIS Admin Portal.

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.

* A complete list of permissions is kept on file in the technology department.