Nashua School District

Data Governance Plan

May, 2020

Contents

Background

In June 2018, the New Hampshire State Legislature passed, and Governor Chris Sununu signed into law, House Bill 1612. This is a new mandate for the Department of Education. New Hampshire Public Schools, including the Nashua School District, are tasked with developing a data governance manual. The implementation timeline for presentation and approval of an initial plan was limited to one year only after House Bill 1612 was signed into law.

Creation of this plan has been dependent on resources from the New Hampshire Department of Education, FERPA, CIPA and COPPA (including data and security standards), not finalized until April

Purpose

The Nashua School District provides its faculty, staff, and administrative staff access to technology devices, software systems, network and Internet services to support research and education. All components of technology must be used in ways that are legal, respectful of the rights of others, protective of juveniles and promote the educational objectives of the 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 Nashua 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.

Scope

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

- Speech, face to face communications, phone communications or any current and future technologies.
- Hard copy data (printed or written).
- Communications sent by post/courier, fax, electronic mail, text, chat and/or any form of social media.
- Data stored and/or processed by any electronic device, including: servers, computers, tablets, and mobile devices.
- Data stored on any type of internal, external, or removable media or cloud based service.

Note:

- 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 Nashua School District and shall be protected from misuse, unauthorized manipulation, and destruction.

Regulatory Compliance

employment and others. The District will collect, create or store confidential information only when the Superintendent or designee determines it is necessary.

New Systems

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

The Nashua School District has an established process for vetting new digital resources. Staff are required to complete steps outlined as follows:

-

all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage.

Data managers will:

- ensure that system account creation procedures and data access guidelines appropriately match staff member job function with the data on instructional and operational systems.
-

When possible, the District will limit the number of concurrent sessions for a user account in a system.

Remote Access

also have a mapped personal folder. This folder acts as a redirection of document and desktop folders to

- Additional training for new instructional staff on the use of digital resources and student electronic records.

Archival and Destruction

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

District Data Destruction Processes

The District will regularly review all existing data stored on district provided storage for the purposes of

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

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 maid ˜ biometric r
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 Psg-3(s)71(n hpaeF>>5004(se)p)17(ny)-4(-)5(i) a11(a) securiat a1 satN(se)pmas

- NH RSA 189:66 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-66.htm) Data Inventory and Policies Publication
- NH RSA 189:67 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-67.htm) Limits on Disclosure of Information
- NH 189:68 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68.htm) Student Privacy
- NH RSA 189:68-a (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68-a.htm) Student Online Personal Information

New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data[21]

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

- NH RSA 359-C:19 (http://www.gencourt.state.nh.us/rsa/html/Nashuai/359-c/359-c-19.htm) Notice of Security Breach - Definitions
- NH RSA 359-C:20 (http://www.gencourt.state.nh.us/rsa/html/Nashuai/359-c/359-c-20.htm) Notice of Security Breach Required
- NH RSA 359-C:21 (http://www.gencourt.state.nh.us/rsa/html/Nashuai/359-c/359-c-21.htm) Notice of Security Breach Violation

Appendix C - Digital Resource Acquisition and Use

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

-

- and minimize malicious code that can be inadvertently downloaded.

New Resource Acquisition

Staff are required to complete an application review process, which is currently under development. An online request form is required for any new digital resources that either has an associated cost or collects staff or student data. All staff must adhere to the following guidelines regarding digital resource acquisition:

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

Approved Digital Resources

In order to ensure that all digital resources used meet security guidelines and to prevent software

an evaluation of the information assets and the technology associated with its collection, storage, dissemination and protection.

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

Data Security Checklist for District Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)
- Physical security of system
- Location within network including network systems protection (firewall, content filter) and if system is externally facing or only allows for district network access
- Access controls including password security (can district password requirements be enforced)
- Authentication methods (LDAP/Active Directory, Single Sign On, district managed account, user managed account)
- Server/system security patch frequency
- Ability to access from mobile devices
- Ability to maintain critical system event logs
- Ability to receive notification for critical system events

Data Security Checklist for Provider Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)
- Contract, terms of service and privacy policy are current and meet district data security requirements

Appendix E - Data Classification Levels

Personally Identifiable Information (PII)

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

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

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

Confidential Information

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

Unauthorized disclosure of this information to individuals without a business need for access may violate

Appendix F - Securing Data at Rest and Transit

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 3rd 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.

Appendix G

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 Nashua 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

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

Virus, Malware, and Spyware Protection

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

Internet Filtering

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

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing using third-party services.

Security Patches

Server patch management is performed regularly. Security patches are applied on an as needed basis.

Appendix J - Account Management

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

Staff Accounts

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

- Notification of new staff member is sent from Human Resources to the Technology Department. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology Department creates user accounts. The user is given access and permissions to the necessary

All VPN accounts will be reviewed at least annually.

In lieu of recent events relating to the Covid-19 pandemic, Remote Desktop Services has been granted to District leadership, building leadership and their administrative staff to ensure the District continues to operate as “business as usual.”

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractors/vendor access must be approved by HR and ISO. All contractors doing business on district premises must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing district data will be considered on premise users. Once the approval has been obtained, the technology department will create the account.

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

Staff are entered into the Nashua 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

- Specials_RO
- SRO
- Unassigned - no access

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

Financial System

All staff members are entered into the District’s financial system for the purpose of staff payroll and HR

- IEP Team Member
- District Administrator
- SAU System Administrator
- SAU System Staff
- General Ed Teacher
- SAU District Administrator

Appendix L - Password Security

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable the Nashua 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.

Planning Assumptions

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

- There may be natural disasters that will have greater impact than others.
-

- The District’s data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and the cloud. The District’s critical virtual servers can be run directly from the cloud with limited access.
- In the event of a critical system failure, the District can restore that server back to our current environment from the backup solution.

Deactivation

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

Evaluation

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

Appendix N - Data Breach Response Plan

Objectives

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

- Data inventory of all systems containing sensitive data will be secured by the Department of Technology.
- Data dictionary of all district hosted information systems Due to non- disclosure agreements, this data may not be available in will be secured by the Department of Technology. The appropriate vendor(s) can be contacted for this information.
- Maintained spreadsheet listing all server names, physical and virtual, and their function.
- 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 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.