2023

DATA GOVERNANCE PLAN

2023

Introduction

The terms "data" and "information" are used interchangeably throughout the Data Governance Plan (DGP). "Data" is defined as fact or information in any form: oral, written or electronic. All standards that address data security are located in the Goffstown School District's confidential District Security Plan (DSP).

The Goffstown School District (GSD) is committed to maintaining strong privacy and security protections. It is the practice of the GSD that data and/or information in all forms written, electronic, or printed be protected from intentional, accidental, or unauthorized modification, destruction, or disclosure. Protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information. This DGP formally outlines how operational and instructional activity shall be carried out to make certain that GSD student and employee data are accurate, accessible, consistent, and protected. The DGP establishes who is responsible for data and/or information under various circumstances and specifies what procedures, policies, standards, and/or practices shall be used to manage and protect it.

Purpose

The purpose of GSD technology is to advance the educational opportunities and achievement for all students and to support efficient management and processing of district-related functions. Technology also supports professional skillsets and staff knowledge and increases engagement of families and other stakeholders in the educational community, which positively impacts student achievement.

Compliance with laws mandating confidentiality, maintaining the trust of the district's stakeholders and accurately maintaining and protecting confidential data is important for efficient GSD operations. All persons who have access to GSD data are required to follow federal and state law; moreover, all employees and authorized contractors or agents using Personally Identifiable Information and/or Confidential Information will strictly observe protections put into place by the GSD through policy, procedures, standards and practices.

Scope

All data policies, standards, processes and procedures apply to students, employees of the district, contractual third parties, agents of the district, and volunteers who have access to district data or systems. This DGP applies to all forms of data and information including but not limited to:

1. Speech, spoken or communicated by phone or any current and future technologies.
2. Hard-copy data, printed or written.
3. Communications sent by post/courier, fax, electronic mail, text, chat, and/or any form of social media.
4. Data stored and/or processed by any electronic device, including servers, computers, tablets, and mobile devices.
5. Data stored on any type of internal, external, or removable media or cloud-based service.
6. 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 that may be referred to as "systems," "assets" or "resources."

All involved systems and information are considered GSD assets and shall be protected from misuse, unauthorized manipulation, and destruction.

Regulatory Compliance

The district will abide by any legal, statutory, regulatory, or contractual obligations affecting its data systems. (Appendix B) The GSD complies with or exceeds the NH Minimum Standards for Privacy and Security of Student and Employee Data approved in 2019, and standards applicable to data governance are addressed throughout this Data Governance Plan. The GSD complies with all other applicable regulatory acts, including (but not limited to):

- Children's Internet Protection Act (CIPA)
- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Pupil Rights Amendment (PPRA)
- Individuals with Disabilities in Education Act (IDEA)
- New Hampshire State RSA - Student and Teacher Information Protection and Privacy
    - NH RSA 189:65 Definitions
    - NH RSA 189:66 Data Inventory and Policies Publication
    - NH RSA 189:67 Limits on Disclosure of Information
    - NH 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

Data User Compliance

The Data Governance Plan applies to all users of GSD information, including staff, students, volunteers, and authorized contractors and agents. All data users are to maintain compliance with School Board Policies and GSD administrative procedures, EHAB (Data Governance and Security), GBEF (Network and Internet Acceptable Use Policy), GBEF-R (Network and Internet Acceptable Use Regulations), JICL (Network and Internet Acceptable Use Policy), JICL-R (Network and Internet Acceptable Use Regulations) and all policies, procedures, and resources as outlined within this plan and School Board Policy.

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

Unless permission has been granted by the Director of Technology or designee, no staff, vendor, or other person may remove confidential or critical data from GSD premises or network, remove a device containing confidential or critical data from GSD 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 GSD-provided device with appropriate security controls or through a secure virtual private network (VPN) connection. 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 GSD. The GSD may end business relationships with any contractor who fails to follow the law, GSD policies or procedures, or the confidentiality provisions of any contract. In addition, the GSD reserves the right to seek all other legal remedies, including criminal and civil action and suspension of a staff member's teaching certificate.

The GSD may suspend all access to data or use of its technology resources pending an investigation. Violations may result in temporary, long-term, or permanent suspension of user privileges. The GSD 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 GSD.

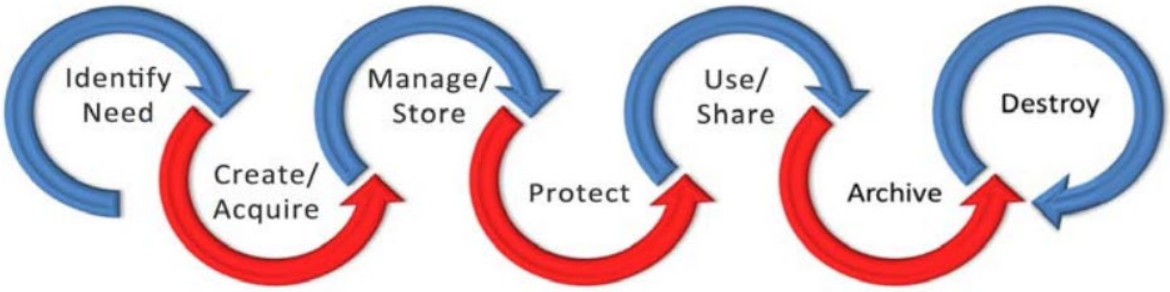
Any attempted violation of GSD policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

Disciplinary/corrective action may be instituted for (but is not limited to) the following:

- Unauthorized disclosure of Personally Identifiable Information (PII) or Confidential Information.
- Sharing of user IDs or passwords (exception for authorized technology support staff).
- Applying for a user ID under false pretenses or using another person's 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.
- Unauthorized copying of files.
- Attempting to secure a higher level of privilege without authorization.
- Installation or use of unlicensed software or software not approved for district technological systems.
- The intentional unauthorized access, altering, destruction, or disposal of district information, data, and/or systems. This includes the unauthorized removal of technological systems 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 or destructive programs.

Data Lifecycle

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



Identifying Need & Assessing Systems for District Requirements

To accomplish the district's mission and to comply with the law, the district may need to maintain Confidential Information, including information regarding students, parents/guardians, staff, applicants for employment, and others. The GSD will collect, create, or store Confidential Information only when the Superintendent or designee determines it is necessary or as required by district policy or law.

Digital Resource Acquisition and Use

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

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

Approved Digital Resources

Digital resources shall be approved by the Director of Technology or designee in order to ensure that they meet security guidelines and prevent software containing malware, viruses, or other security risk.

- The technology department will maintain a list of evaluated software on the GSD Technology site.
- It is the responsibility of staff to submit requests for resource review if a resource is not listed.
- Resources that are labeled "denied" or have not yet been reviewed will not be allowed on GSD devices or used as part of business or instructional practices.

Digital Resource Licensing/Use

All computer software developed by GSD employees or contract personnel on behalf of the district or licensed or purchased for its use is the property of the GSD 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 GSD resources are to be used.
- GSD 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 GSD systems and other electronic devices will have a current license on file or will be removed from the system or device.

- Digital resources that are accessed from and/or that store data in a cloud environment will have a memorandum of understanding (MOU) or contract on file that states or confirms at a minimum that:
    - Student and/or staff data will not be shared, sold, or mined with or by a third party.
    - Student and/or staff data will not be stored on servers outside the US.
    - The provider will comply with GSD guidelines for data transfer or destruction when contractual agreement is terminated.
    - No Application Programming Interface (API) will be implemented without full consent of the GSD.
    - 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. (Appendix M)
- Resources with or without physical media (e.g. downloaded from the Internet, apps, or online) shall still be properly evaluated 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 the Director of Technology or designee.

New Resource Acquisition

New resources are defined as (but not limited to) online curriculum resources, library subscriptions, and software applications. A software resource request form [found online under staff technology resources in the GSD Learning Management System (LMS)] is required for any new digital resources that either have an associated cost or collect any 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 Director of Technology prior to initiation.
- Before requesting use of any tool, it is the responsibility of staff to ensure that all electronic resources are age appropriate, both FERPA and COPPA compliant, and compliant with software agreements. No autonomous listening devices or personal assistants with listening and/or recording devices (such as Echo, Alexa, Google Assistant, Apple HomePod, Siri, etc.) are to be allowed in any school buildings.
- It is the responsibility of the staff requesting digital content to properly vet the resource to ensure that it meets GSD business objectives, is in line with curriculum or behavioral standards, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional materials will be vetted by the appropriate Assistant Superintendent and the Director of Technology, or designee, prior to purchase.

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

- Impact on technology environment, including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements, including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Staffing resources required to roster and support the system
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:

- Student and/or staff data will not be shared, sold, or mined with or by a third party.
- Student and/or staff data will not be stored on servers outside the US.
- The provider will comply with GSD guidelines for data transfer or destruction when contractual agreement is terminated.
- No API will be implemented without full consent of the GSD.
- 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. (Appendix M)
-

Management and Storage

Systems Security

The GSD will provide access to Confidential Information to appropriately trained staff and volunteers only when it determines that such access is necessary for the performance of their official duties. The district will disclose Confidential Information only to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law and authorized by the GSD (School Board Policy EHAB). Therefore, system access will only be given on an as-needed basis as determined by the Superintendent or his/her designee. Further information regarding Data Access Security Controls is contained in the Security/Protection section of this data governance plan.

Data Management

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

All GSD administrators are Data Managers for all data collected, maintained, used, and disseminated under their supervision, as well as data they have been assigned to manage. Data Managers are responsible for the development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. Data Managers will:

• only create or maintain Personally Identifiable Information (PII) within the personnel file that is secured and protected or essential for retention.

• ensure that system-account creation procedures and data-access guidelines appropriately match staff member job function.

• review all staff with custom data access beyond their typical group's access.

• review GSD processes to ensure that data will be tracked accurately.

• review contracts with instructional and operational software providers to ensure that they are current and meet GSD data-security guidelines.

• ensure that staff are trained in proper procedures and practices in order to ensure accuracy and security of data.

• assist the Director of Technology in enforcing district policies and procedures regarding data management.

Data Classification and Inventory

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected in all formats. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data is

classified according to the most sensitive detail they include. Data recorded in several formats (e.g. source document, electronic record, report) have the same classification regardless of format (Appendix D).

The Director of Technology or designee will identify all systems containing district data, such as personnel files, network and local files, student information systems, financial systems, human resources systems, payroll systems, transportation systems, food-service systems, email systems, instructional software applications, and others. Once the data files and data elements are identified, the Director of Technology or designee will classify the data as confidential or critical so that those files and the information they contain can be more closely monitored.

The GSD will create and maintain a data inventory for all digital information systems containing PII and/or Confidential Information. When possible, a data dictionary will be maintained for Critical Information systems. The data inventory will contain the following elements:

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

Security/Protection

Risk Management

A thorough risk analysis of all GSD data networks, systems, policies, and procedures shall be conducted in accordance with GSD Security Policy. An internal audit of GSD network security will be conducted annually by Technology staff.

Security Logs

In accordance with its Security Plan, the GSD will maintain a comprehensive list of critical system events that will be logged and monitored to ensure data security. These events will include (but are not limited to) access to critical systems and modification of Critical Data. When applicable, notifications will be established for critical event triggers.

Physical Security Controls

Technology telecommunication closets are housed in secure locations. Access authorization is assigned through the Director of Technology and or Director of Facilities. In addition, access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals. (Appendix F)

No technological systems shall be disposed of or moved without adhering to the appropriate procedures. (Appendix G)

Inventory Management

The GSD shall maintain a process for inventory control in accordance with federal and state requirements and School Board policy. All GSD technology assets will be maintained in inventory and verified through the regular inventory verification process. (Appendix G)

Virus, Malware, and Spyware Protection

GSD desktops, laptops, and file servers are protected using enterprise virus/malware/spyware/ or data protection software. Gateway antivirus software is also run on the district firewall. Virus definitions are updated no less than weekly, and an on-access scan is performed on all "read" files continuously. A full scheduled scan is performed on all servers weekly during non-peak hours.

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing as part of our Microsoft Office 365 implementation.

Electronic Access Security Controls

GSD staff will only access Personally Identifiable and/or Confidential Information when necessary to perform their official duties. The GSD will only disclose this information to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law. All staff are required to read and acknowledge applicable district policies.

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

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

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

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

Physical Data Files

All staff and students who generate or maintain Personally Identifiable Information (PII) and/or Confidential Data/Information shall insure the protection and security of these documents. Confidential Data/Information shall be collected, created, stored, or destroyed only when it is deemed necessary and/or as required by law or policy.

Securing Data at Rest and Transit

All staff and students who log into a GSD computer will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on their local GSD-owned device. It is important to note that this data is not a part of the GSD continuity plan, and thus will not be backed up by the GSD backup solution. Staff and students will also have a mapped personal folder. This folder acts as a redirection of document and desktop folders to district file servers. Access to these files is restricted to the folder's owner (staff or student who is assigned) and GSD domain administrator accounts.

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. (Appendix E)

Training

The district shall create and maintain data security training programs. These training programs may be delivered in multiple formats such as digital, face-to-face, workshops, staff meeting presentations, etc.

The programs will require a certificate of completion from all staff. Minimally annual trainings will consist of the following:

- How to identify, secure and protect Confidential Data/Information
- All instructional staff on technology policies and procedures, including confidentiality and data privacy
- All staff on federal regulations and the use of digital resources and student electronic records
- All staff who use data systems shall include data security
- Confirmation that he/she has read the Teacher Technology Handbook
  Other training as deemed appropriate by the Superintendent, or designee, and the Director of Technology

Archival and Destruction

Once data is no longer needed, the Superintendent 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 meet DOD 5220.22-m as the minimum standard which render the record irretrievable. The Director of Technology is authorized to use the GSD procurement process to contract with an independent contractor for records disposal. All departments will adhere to GSD policy and state and federal law for data archival and destruction.

District Data Destruction Processes

The GSD will regularly review all existing data stored on district-provided storage for the purposes of ensuring data identification and appropriate destruction. Data Managers will regularly review systems and data to ensure that data that is no longer needed is destroyed. The following exceptions will be made:

- Data in an active litigation hold will be maintained until the conclusion of the hold.
- Student electronic data will be maintained for one school year after the student's final date of attendance.
- Employee electronic data will be maintained for one year after the final work day, unless HR approves continued GSD administrator access.
- Employment records or personnel files will be destroyed in accordance with GSD policy and/or law.

Asset Disposal

The GSD will maintain a process for physical asset disposal in accordance with School Board Policy DN. The GSD will ensure that all assets containing PII, Confidential, or internal information are disposed of in a manner that ensures the information is destroyed. (Appendix G)

Critical Incident Response

Controls shall ensure that the GSD can recover from any damage to or breach of Critical Data or systems, within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the Director of Technology 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.

Business Continuity

The GSD will maintain systems that provide near-line 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 near-line and off-site backups of critical systems quarterly.

Disaster Recovery

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

Data Breach Response

New Hampshire's data breach law (RSA 359-c:19, 20, 21) is triggered when a GSD 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 GSD to respond effectively and efficiently to a data breach involving Personally Identifiable Information (PII) as defined by NH Law, Confidential or protected information (i.e. that protected by FERPA), or district-identifiable information, or to any 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. (Appendix M)

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 DIRECTOR OF TECHNOLOGY or designee 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.

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.

“Student personally-identifiable data” is defined by the state of NH in RSA 189:65 as:

1. The student's name.
2. The name of the student's parents or other family members.
3. The address of the student or student's family.
4. Indirect identifiers, including the student's date of birth, place of birth, social security number, email, social media address, or other electronic address, telephone number, credit card account number, insurance account number, and financial services account number.
5. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

"Teacher personally-identifiable data" or "teacher data," which shall apply to teachers, paraprofessionals, principals, school employees, contractors, and other administrators, means:

1. Social security number.
2. Date of birth.
3. Personal street address.
4. Personal email address.
5. Personal telephone number.
6. Performance evaluations.
7. Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.
8. Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates

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 Director of Technology 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 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-65.htm) Definitions
- 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

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

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

Appendix C – Data Security

A thorough risk analysis of all GSD data networks, systems, policies, and procedures shall be conducted on an annual basis or as requested by the Superintendent, Director of Technology or designee.

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

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

Data Security Checklist for District Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and nonelectronic)
- 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 (Active Directory, Single Sign On, District managed account, user managed account)
- Server/system security patch frequency
- Ability to stage and test upgrades prior to deployment
- Ability to access from mobile devices
- Ability to maintain critical system event logs
- Ability to receive notification for critical system events
- Backup methods and frequency

Data Security Checklist for Provider Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and nonelectronic)
- Contract, terms of service and privacy policy are current and meet district data security requirements
- Provider has adequate data security measures including data management and incident response
- Ability to ensure proper access controls including password security (can district password requirements be enforced)
- Authentication methods (Active Directory, Single Sign On, District managed account, user managed account)

- Server/system security patch frequency
- Ability to access from mobile devices
- Notification practices in the event of a system compromise or security breach
- Backup method and frequency
- Physical backup locations
- Ownership of data
- Export of data in non-proprietary format at contract termination

Appendix D – Data Classification Levels

Personally Identifiable Information (PII)

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

- Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.

- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

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

Confidential Information

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

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

Internal Information

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

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

Student Directory Information

"Directory Information" relating to a student includes the following:

1. The student's name, address, date of birth
2. Major field of study
3. Participation in officially recognized activities and sports
4. Weight and height of members of athletic teams
5. Dates of attendance
6. Awards and honors received

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.

Appendix E - Securing Data at Rest and Transit

All staff and students that log into a district provided computer will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on their 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. Staff and students will also have a mapped personal folder. This folder acts as a redirection of document and desktop folders to district file servers. Access to these files is restricted to the folder's owner (staff or student who is assigned) and district enterprise administrator accounts.

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

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with both a Google Apps for Education and Office 365 account that provides unlimited storage. Users are responsible for all digital content stored on their district provided accounts. When using cloud storage, staff 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 / Microsoft OneDrive App on Android, iOS, MacOS, and Windows. This will ensure that restrictions applied by the cloud sharing security continue to function properly.
- Data with Personally Identifiable Information of staff or students may not be posted to users' district provided Google Drive, or any other cloud sharing platforms without written consent of district administration. With approval data with PII may be uploaded and accessed ONLY on the district Office 365 platform as long as proper security measures have been taken including restricting access of user data and encryption of the documents.
- 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 district created curricular or operational documentation, files, data, or software applications.
- Staff should never post any documents labeled classified, confidential, or restricted to any cloud storage including district provided Google Drive, and Office 365 accounts without district approval. With approval these documents may be uploaded and accessed ONLY on the district Office 365 platform as long as proper security measures have been taken including restricting access of user data and encryption of the documents.
- 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 employees, students, other Google Apps for Education drive, and other Office 365 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.

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 network storage 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.
- 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.
- When staff leave the district, they must ensure that they delete any district created/provided curricular or operational documentation, files, or data from their personal external storage devices.

File Transmission Practices

- Staff are responsible for securing sensitive data for transmission through email or other channels with encryption or a password.
- Staff should never include a password in any communication with the actual file attached that is being protected by the password.
- Staff should never transmit files labeled classified, confidential, or restricted through email or third-party file transfer services without district approval. Any transfer of these documents must include appropriate security measures including encryption and limiting access and distribution.
- Regular transmission of student data to services such as a learning management 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 Instructional Technology.

Credit Card and Electronic Payment

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

level of PCI compliance when handling such data:

- Never store cardholder data on district systems or in written form. All cardholder data may only be entered in secured payment systems approved by the district. Any cardholder data collected in written form must be shredded immediately after entry into 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 F - Physical Security Controls

The district will implement best practices in physical security. The details are specified in the DSP.

The following physical security controls shall be adhered to:

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

Appendix G - Asset Management

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

All resources purchased with grant funds will be managed in accordance with federal and state compliance requirements. The Director of Technology will work with the SAU 19 Administration to ensure compliance.

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

Inventory

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

Disposal Guidelines

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

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

The Director of Technology shall approve disposals of any district technology asset. Documentation of the asset disposal will include the asset tag number (if different from the serial number), description, serial number and method of disposal.

Methods of Disposal

Once equipment has been designated and approved for disposal, 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.

Salvage

All technology assets shall be salvaged in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium. 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

In the event that the district determines that an asset shall be donated, an MOU must be approved by the Business Administrator. Since 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. In addition, software licenses are not transferred outside the district. Therefore, systems must be returned to factory installation prior to donation.

Asset Disposal

The district will maintain a process for physical asset disposal in accordance to Board policy. The district will ensure that all assets containing PII, confidential, or internal information are disposed of in a manner that ensures that this information is destroyed.

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

Virus, Malware, and Spyware Protection

GSD desktops, laptops, and file servers are protected using enterprise virus/malware/spyware/ or data protection software. Gateway antivirus software is also run on the district firewall. Virus definitions are updated weekly, and an on-access scan is performed on all "read" files continuously. A full scheduled scan is performed on all servers weekly during non-peak hours.

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing as part of Office 365.

System Updates, Upgrades and Security Patches

Server and system updates are to be reviewed and applied at least quarterly. System updates are to be tested on a staging environment before being pushed into production. Upgrades for critical systems are to be performed during times of low network volume such as school vacations. Security patches are applied on an as needed basis. Any update that may result in a network outage should be announced in advanced whenever possible and documented on the online system outage calendar

Appendix I – Account Management

Access controls are essential for data security and integrity. The Goffstown 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.

Employee Accounts

Access controls are essential for data security and integrity. Goffstown School District maintains a strict process for the creation and termination of district accounts. All new employee accounts are authorized through a Human Resources 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.

New Hires

When an employee is hired by the Goffstown 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 employee is sent from Human Resources to the Technology Department. This notification includes position, building assignment(s), employee ID, and start date. New employees will not be provided with log-in accounts to systems, district email, or with district-owned devices until their official hire date unless approved by both the Director of Technology and the Superintendent.
- Only after notification has been received from Human Resources, the Technology Department creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s)
- Any exception to permissions must be approved by the Director of Technology, and the Assistant Superintendent or Superintendent. This request must use the Additional Access Request form.

Terminations

When a staff member's employment is ended, either by termination or resignation, account permissions are revoked in one of two ways.

- In the event of termination, HR will send immediate notification via email or phone call to Technology leadership requiring the account to be disabled at once, preventing any further access to district resources. HR will also send a Suspension of Service showing the termination date.
- In the event of resignation, HR sends a Suspension of Service to Technology, indicating the termination date. The account is disabled at the end of business on the termination date, preventing further access to district resources.
- In the event that a user having elevated permissions to any system separates from the district, additional measures are taken to ensure that all elevated accounts to those systems are secure.
- In all instances, the system account and associated network storage of the user that has separated from the District are immediately deactivated on the termination date.

Extended Leave

When a staff member takes an extended leave of absence from the district, accounts will be disabled, and the all district owned equipment must be turned in to be re-appropriated to the replace or to the area of need as determined by the Director of Technology.

Volunteers / Interns / Student teachers

Volunteers/Interns/Student teachers and others as determined, will be provided with log-in accounts to the following district systems: network login, Office 365, and Google Applications. These users will NOT be given access to systems containing PII, or be eligible to be assigned district-owned devices. An exception may be made with approval by the Director of Technology and the Superintendent.

Vendors (including consultants and contracted service providers) and contractors

Vendors and contractors who are performing services for the district will be provided with log-in accounts to the following district systems: network login, Office 365, and Google Applications. These users will only be provided access to systems containing PII when required to complete their assigned duties. These users can choose to either use a district-owned device or use their own as long as they provide documentation of compliance with the security standards defined in Appendix O . Exceptions may be made with approval by the Director of Technology and the Superintendent.

Local/Domain Administrator Access

No user, with the exception of the technology department staff, will be granted administrative or super-user access to any server level system. Access will be restricted to the lowest level necessary to perform specific job functions. Local administrator rights on end user devices may be allowed under certain conditions when deemed necessary by the Director of Technology.

Remote Access

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

In the event that VPN access is needed by a contractor/vendor, access must be approved by the Director of Technology. The Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports. All VPN connections will require 2FA as a second layer of authorization to validate the connecting user.

In the event that a vendor/contractor needs access to a public facing system (SIS, LMS, Heating, POS, etc.), a user account will be created, and access will be provided upon approval of the Director of Technology and the Superintendent. Access will be provided using a standard web interface.

It is the remote user's responsibility to ensure that the remote network is capable of establishing a VPN connection with the District's network.

All VPN accounts will be reviewed by the Director of Technology at least annually.

Remote control to internal systems for the purpose of support and maintenance must be approved in advance by the Director of Technology or his/her designee.

Appendix J – Data Access Roles and Permissions

Student Information System (SIS) [Powerschool]

All staff members are entered into the District's SIS as the primary data source for synchronization to other district managed online systems. Only staff requiring access are provided accounts for the system. The following minimal information is entered for each staff member:

- Employee Name, ID Number
- Staff Type
- Status - Active
- Position
- Alert System Contact Phone Numbers

System access is granted by the PowerSchool Administrator or Director of Technology when the user is granted district network privileges and training is provided. SIS logins are synchronized with user's network logins for authentication (SSO).

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 District Student Data Manager. 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. Administrative accounts log into the SIS Admin Portal.

SIS Security Groups

- Administrator (SIS)
- Admin with Scheduling
- Counselors No Scheduling
- Data Management and DDE
- Demo-Schedules
- Demo-Sched-Quick Lookup
- Food Service Mgr
- High School Counselors
- Media Specialists
- Nurses
- Office Attd-Demo View Only
- Office Attendance Sub
- Office Staff Attd & Discipline
- Office & Sped View Only
- Principal-Admin
- Quick Lookup-Log Entries
- Registrar with Scheduling
- Registrar without Scheduling

- SAU Staff
- Schedules and Attendance

Student Information Access

A. Alerts (Fees, Guardian, Other)
    - View: Teachers, All Admin Portal Users
    - Maintain: Secretaries
B. Alerts (Medical)
    - View: Teachers, All Admin Portal Users
    - Maintain: Nurses
C. Attendance including attendance codes, in/out times and total counts
    - View: Administrators, Counselors, Nurses, Teachers, Secretaries
    - Maintain: Designated Secretaries
D. Demographics & Emergency Contacts
    - View: Administrators, Counselors, Nurses, Teachers, Secretaries
    - Maintain: Designated Secretaries
E. Fees
    - View: Administrators, Counselors, Secretaries
    - Maintain: Designated Secretaries
F. Gradebook Grades/Assessments (assignments, tests, finals, etc.)
    - View: Administrators, Counselors, Teachers, Secretaries
    - Maintain: Teachers, Designated Secretaries
G. Historical and Transfer Grades
    - View: Administrators, Counselors
    - Maintain: Designated Secretaries
H. Log Entries - Discipline
    - View: Administrators, Counselors, Secretaries
    - Maintain: Designated Secretaries
I. Schedules
    - View: Administrators, Counselors, Nurses, Teachers, Secretaries
    - Maintain: Counselors, Designated Secretaries
J. Test Results
    - View: Administrators, Counselors, Teachers (Specific Report Templates)
    - Maintain: District Student Data Manager, Designated Secretary

Student Medical Information

A. Medical data includes Immunizations, Screenings, Allergies, Conditions, Medications, Medical Alerts, Office Visits, Doctor & Dentist, Nurse Notes
B. School nurses are the only accounts that can VIEW & MAINTAIN ALL medical information.
C. Viewable Emergency Information (Allergies, Conditions, Doctor & Dentist) - Administrators, Counselors, Service Providers, Secretaries
D. Viewable Medical Alerts – All Admin Portal Users & Teacher Portal Users

Learning Management System (LMS) [Schoology]

All student and staff members are imported into our LMS. Access in our learning management system is determined by user role and responsibility. The LMS stores the following information about a user:

- First and Last Name
- SSO user name
- Student / Employee internal id number
- Primary school assignment
- Job class (Student / teacher / support staff / administrator / etc)
- Email address
- Assessment data for users (quiz scores, submitted assignments, etc)

Access within the LMS is assigned using the principle of least privilege.

- Teachers can only access courses that they are teaching (present or historical). They have the ability to add and remove students and add additional staff members with limited read permissions.
- Students can only read and participate in their current courses
- School Administrators can read, access, and edit courses and content within their respective schools
- District administrators can read, access, and edit courses and content through-out the district as specified by their role
- Parents can access current academic classes of their child and have a limited view of the content.

LMS Access Roles:

- System Administrator – Has the ability to manage the LMS server instance.
- Teacher – Has the ability to view, edit, access, and create content in assigned courses and groups.
- Student – Has the ability to view and participate in assigned courses and groups. These students can also use the instant-messaging system built into the LMS
- K-8 Student - Has the ability to view and participate in assigned courses and groups.
- School / District Admin – Has the ability to view, edit, and access courses and groups that have been created at their corresponding schools
- ParaEducator – Has the ability to view content of assigned courses and groups. These users also have the ability to view student progress of assigned students.
- Guidance / Student Support – Has the ability to view content of assigned courses and groups. These users also have the ability to view student progress of assigned students.
- No-Access – Can log into the LMS, but have no access to courses or groups.
- Parent – Has the ability to view courses or groups that are assigned to their child. They can also view the progrerss of their child.

Employee / Professional Development Portal [Moodle]

All employees are imported into our employee and professional development portal. Access in our PD system is determined by user role and responsibility. The PD portal stores the following information about a user:

- First and Last Name
- SSO user name
- Employee Identification number
- Primary school assignment
- Job class (Student / teacher / support staff / administrator / etc)
- Email address
- Assessment data for users (quiz scores, submitted assignments, etc)

Access within the PD Portal is assigned using the principle of least privilege.

- Trainers can only access courses that they are teaching (present or historical). They have the ability to add and remove staff and add additional trainers with limited read permissions.
- Participants can only read and participate in their current courses
- School administrators can read and pull report about the progress of staff from their corresponding school building.
- SAU administrators can read, access, and edit training courses and content through-out the site as specified by their role

PD Portal Access Roles:

- Administrator – Has the ability to manage the PD server instance.
- Manager – Has the ability to manage aspects of the PD portal including creating and managing courses
- Supervisor – Has the ability to view, edit, and access courses. This role has the same functionality as a teacher / trainer but does not receive email notifications. This role has the ability to pull reports from the system.
- Teacher / Trainer– Has the ability to view, edit, access, and create content in assigned courses.
- Non-editing teacher / Non-editing trainer– Has the ability to view and access assigned courses.
- Student / participant– Has the ability to view and participate in assigned courses.

Special Education System [NHSEIS]

The State of New Hampshire provides the District access to the NH Special Education Information System (NHSEIS) that houses all student IEP information. Access accounts to NHSEIS is maintained by the District's Director of Special Education office through the MyNHDOE single sign on portal. A user role determines the user's authority and applicable permissions within the NHSEIS system. The established roles are as follows:

- School Administrator
- Provider
- Case Manager
- District IT Administrator
- IEP Team Member
- District Administrator
- SAU System Administrator
- SAU System Staff
- General Ed Teacher
- SAU District Administrator

The following user roles access NHSEIS through the MyNHDOE portal: Case Manager, District Administrator, District IT Administrator, SAU District Administrator, SAU System Administrator, SAU System Staff, and School Administrator. The remaining user roles, Provider, General Ed Teacher and IEP Team Member access NHSEIS through a SAU specific web address.

Food Services System [Titan]

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

Food Services System Roles:

- Administrator
- Cashier
- Head cook

Financial System [eFinance]

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.

Financial System Security Roles:

Although we do not have defined roles established in E-finance, we do use resources to segment users by the functionality they require to perform their jobs. Specifically, we have five defined "resources" as follows:

1. Business Office and HR employees – almost all functionality
2. Principal Secretaries – includes budget, payroll and purchasing
3. Secretaries – purchasing only
4. Administration – purchasing approvals
5. Treasurers – payroll and accounts payable approvals.

Appendix K - Password Security

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

- Passwords shall never be shared with another person.
- When possible, user created passwords should adhere to the same criteria as required for district network access as outlined below.
- Passwords shall never be saved when prompted by any application with the exception of single sign-on (SSO) systems as approved by the Technology Department.
- Passwords shall not be programmed into a PC or recorded anywhere that someone may find and use them.
- When creating a password for secure information or sites, it is important **not** to use passwords that are easily guessed due to their association with the user (i.e. children's names, pets' names, or birthdays).
- Users and employees who have reason to believe a password is lost or compromised must notify the Director of Technology or designee as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

District network access to resources managed through Active Directory/SSO:

- Passwords must be "strong," meeting the following minimum complexity requirements:
  - At least eight (8) characters in length
  - At least one (1) uppercase letter
  - At least one (1) lowercase letter
  - At least one (1) special character
  - At least one (1) number
- You will not be allowed to use your previous password.
- Your password must not contain your username, first name or last name.

Where possible, system software should enforce the following password standards:

- Passwords routed over a network shall be encrypted.
- Passwords shall be entered in a non-display field.
- System software shall enforce the changing of passwords and the minimum length.
- System software shall disable the user password when more than five consecutive invalid passwords are given. Lockout time shall be set at a minimum of 10 minutes.
- System software shall limit user accounts to a maximum of 5 concurrent (simultaneous) logins. Additional login attempts should either be rejected or terminate the oldest of the concurrent connections.
- System software should maintain a history of previous passwords and prevent their being easily guessed due to their association with the user.

Appendix L - Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable Goffstown School District (GSD) 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 GSD TDRP:

- 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 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

GSD has appointed the following people to the disaster recovery/critical failure team: The Director of Technology, Network Administrators, all Technician IIs, and the District Student District Student Data Manager.

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

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

Activation

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

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

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

Notification

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

- Superintendent
- Superintendent's Leadership Team (SLT)
- Technology Staff
- District Employees
- 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
- SMS (Text Message)
- Radio or Television

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

Implementation

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

- Maintained spreadsheet listing all server names (servers.xlsx), physical and virtual, and their function. A hard copy of this document will be secured at the technology office and the Assistant Superintendent of Support Services office. An electronic version will be housed on Office 365.
- Maintained spreadsheet of all local administrator accounts, passwords and vendor contact information. A hard copy of this document will be secured at the technology office and the Assistant Superintendent of Support Services office. An electronic version will be housed on Office 365.
- 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 to the data bunker. 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 GSD 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 M - Data Breach Response Plan

Objectives

The purpose of the Technology Data Breach Plan (TDBP) is to enable Goffstown School District GSD 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 TDBP are:

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

Planning Assumptions

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

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

Data Breach/Incident Response Team

GSD has appointed the following people to the data breach/incident response team: The Director of Technology, Network Administrators, all Technician IIs, and the District Student Data Manager.

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

- Determine the nature of the data compromised and its impact to staff, students and the district itself.
- Communicate impact, the number of affected individuals, the likelihood information will be or has been used by unauthorized individuals and updates of progress to the District Superintendent.
- Coordinate with Superintendent to ensure communication with district staff and or parents as deemed appropriate.
- Oversight of the TDBP implementation and data breach resolution.
- Allocate and manage technology staff resources during the event.
- Work with vendors, 3rd party providers, manufacturers, legal counsel, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Oversight of TDBP implementation debrief.

Activation

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

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

- Confidential or sensitive data has been compromised.
- Network hack/intrusion has occurred.

The Director of Technology or designee will act as the incident response manager (IRM). If the Director of Technology 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 District policy EHAB, state, and federal requirements. The Director of Technology will work with the Superintendent of schools to dispense and coordinate the notification and public message of the breach.

Notification

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

- Superintendent
- Superintendent's Leadership Team (SLT)
- Technology Staff
- District Employees
- Parents and Students
- Vendors

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

- Email
- Social Media
- Radio or Television
- First Class Mail
- SMS (Text Message)
- Phone

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

Implementation

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

- Data inventory of all systems containing sensitive data. A hard copy of this document will be secured at the technology office and the Assistant Superintendent of Support Services office. An electronic version will be housed on Office 365.
- Data dictionary of all district hosted information systems. A hard copy of this document will be secured at the technology office and the Assistant Superintendent of Support Services 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 (servers.xlsx), physical and virtual, and their function. A hard copy of this document will be secured at the technology office and the Assistant Superintendent of Support Services office. An electronic version will be housed on Office 365.
- Maintained spreadsheet of all system administrator accounts, passwords and vendor contact information. A hard copy of this document will be secured at the technology office and the Assistant Superintendent of Support Services office. An electronic version will be housed on Office 365.

- 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.

The following will take place during the incident response:

- The members of the IRT will be assembled once a breach has been validated. The IRT will be comprised of: The Director of Technology, Network Administrators, all Technician IIs, and the District Student Data Manager. Additional members of the GSD 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 on-going breach, the IRT will initiate appropriate measures to prevent further data loss. These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.
- The IRT will work with the Data Managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
- The IRM will work with legal counsel and the Superintendent's Leadership Team to determine appropriate course of action pursuant to state statute. This includes notification of the authorities, local law enforcement, and the New Hampshire State Attorney General.
- 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 GSD Communications department 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.
- Once the incident response team has determined the severity of the breach, the team will notify the IRM to determine whether or not the Family Policy Compliance Office (FPCO) or PTAC needs to be notified.
- 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 District policy EHAB. 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 will be maintained for five years.

Deactivation

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

Evaluation

Once the breach has been mitigated an internal evaluation of GSD TDBP response will be conducted. The IRT, in conjunction with the IRM and others that were involved, will review the breach and all mitigation

steps to determine the probable cause(s) and minimize the risk of a future occurrence. Feedback from the responders and affected entities will be incorporated into an after-action report and corrective action plan. The result will be an update to the TDBP and other emergency response plans as appropriate. Information security training programs will be modified to include countermeasures to mitigate and remediate previous breaches so that past breaches do not recur. The reports and incident review will be filed with all evidence of the breach.

Appendix N – Data Security Requirements for Contracted Service Providers

NH RSA 189:66 defines minimum data security standards for the safe handling of student and employee data. Any contractor who is providing services for the district will ensure that any system accessing or storing student or employee personal identifiable information as defined in Appendix A meets or exeeds the minimum security standards below.

1. The Service Provider will review the list of any technology and platforms or applications that he/she intends to use to provide the services against the registry of the district approved technology platforms available on the District's website. If the technology/platform/application is not listed in the District registry, the service provider will ensure ensure that technology/platform/application adheres to the data security requirements below. If any technology/platforms/applications do not meet these requirements, the Service Provider will find a suitable alternative
2. The Service Provider will secure usernames, passwords, and any other means of gaining access to the Services in accordance with industry standards. The Service Provider will implement and maintain reasonable security procedures and practices appropriate to the nature of District covered information, and protect that information from unauthorized access, destruction, use, modification, or disclosure.
3. When the Service Provider is using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Service Provider shall host data pursuant to the Agreement in an environment using a firewall that is periodically updated according to industry standards
4. The Service Provider agrees to the following privacy and security standards for his or her own technology, equipment, and platforms/applications from "the Minimum Standards for Privacy and Security of Student and Employee Data" from the New Hampshire Department of Education. Specifically, the Contractor / service provider must meet the folling requirements:

    i. Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

    ii. Limit unsuccessful logon attempts;

    iii. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

    iv. Authorize wireless access prior to allowing such connections;

    v. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

    vi. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

vii. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

viii. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

ix. Enforce a minimum password complexity and change of characters when new passwords are created;

x. Perform maintenance on organizational systems;

xi. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

xii. Ensure equipment removed for off-site maintenance is sanitized of any District Confidential Information in accordance with NIST SP 800-88 Revision 1;

xiii. Protect (i.e., physically control and securely store) system media containing District Confidential Information, both paper and digital;

xiv. Sanitize or destroy system media containing District Confidential Information in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

xv. Control access to media containing District Confidential Information and maintain accountability for media during transport outside of controlled areas;

xvi. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

xvii. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

xviii. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

xix. Protect the confidentiality of District Confidential Information at rest;

xx. Identify, report, and correct system flaws in a timely manner;

xxi. Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

xxii. Monitor system security alerts and advisories and take action in response; and

xxiii. Update malicious code protection mechanisms when new releases are available.

Alternatively, the Service Provider meets or complies with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Contractor will provide to the District on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

In the event that District Confidential Information is accessed or obtained by an unauthorized individual, The Service Provider shall provide notice to the District as soon as practicable and no later than within ten (10) days of the incident of the following information:

i. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
ii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iii. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
iv. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
v. The estimated number of students and staff affected by the breach, if any.

Any exceptions to this above policy need to defined in writing and approved by the Director of Technology and the Superintendent.

Appendix O: Data security requirements for a contractor or service provider to gain access district systems.

NH RSA 189:66 defines minimum security standards for the safe handling of student data. Any contractor or service provider who is providing services for the district will ensure that any system accessing or storing student or employee personal identifiable information as defined in Appendix A meets or exeeds the minimum security standards below:

Contractor or service providers who are are looking to access any district system (whether it contains PII or not), must have reviewed and agreed to the district's Acceptable use Policy (Policy GBEF & GBEF-R). They must also have reviewed and completed the districts confidentiality agreemnent.

Any contractors or service providers accessing district systems will ensure that their employees will only use District provided technology, equipment, and platforms/applications to provide the Services. Alternatively, the Contractor or Service Providers may be allowed to use his or her own technology, equipment, and platforms/applications assuming the following conditions:

A. The Contractor or Service Provider will secure usernames, passwords, and any other means of gaining access to the Services in accordance with industry standards. The Service Provider will implement and maintain reasonable security procedures and practices appropriate to the nature of District covered information, and protect that information from unauthorized access, destruction, use, modification, or disclosure.
B. When the Contractor or Service Provider is using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. The Contractor or Service Provider shall host data pursuant to the Agreement in an environment using a firewall that is periodically updated according to industry standards
C. The Contractor or Service Provider agrees to the following privacy and security standards for his or her own technology, equipment, and platforms/applications from "the Minimum Standards for Privacy and Security of Student and Employee Data" from the New Hampshire Department of Education. Specifically, the Contractor agrees to:

    i. Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
    ii. Limit unsuccessful logon attempts;
    iii. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
    iv. Authorize wireless access prior to allowing such connections;
    v. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
    vi. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

vii. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
viii. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
ix. Enforce a minimum password complexity and change of characters when new passwords are created;
x. Perform maintenance on organizational systems;
xi. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
xii. Ensure equipment removed for off-site maintenance is sanitized of any District Confidential Information in accordance with NIST SP 800-88 Revision 1;
xiii. Protect (i.e., physically control and securely store) system media containing District Confidential Information, both paper and digital;
xiv. Sanitize or destroy system media containing District Confidential Information in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
xv. Control access to media containing District Confidential Information and maintain accountability for media during transport outside of controlled areas;
xvi. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;
xvii. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
xviii. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
xix. Protect the confidentiality of District Confidential Information at rest;
xx. Identify, report, and correct system flaws in a timely manner;
xxi. Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
xxii. Monitor system security alerts and advisories and take action in response; and
xxiii. Update malicious code protection mechanisms when new releases are available.

In addition, to the above requirements, the device should meet the following additional district adopted security standards:

i. Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity
ii. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

Alternatively, the Contractor or Service Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS)

Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Contractor will provide to the District on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

D. In the event that District Confidential Information is accessed or obtained by an unauthorized individual, Contractor / Service Provider shall provide notice to the District as soon as practicable and no later than within ten (10) days of the incident of the following information:

i. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
ii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iii. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
iv. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
v. The estimated number of students and staff affected by the breach, if any.

Any exceptions to this above policy need to defined in writing and approved by the Director of Technology and the Superintendent