Hollis School Board
Wednesday, June 5, 2019
Hollis Primary School
6:00 PM
All Times are estimates and subject to change without notice

6:00 Call to Order – Board Chair Mann

6:05 Agenda Adjustments
Approve Meeting Minutes
Nominations/Resignations/Correspondence

6:10 Public Input

6:25 Public Hearing – HSD & SAU Maintenance Trusts and the Water System Trust

6:45 Hollis Administrations End of Year Presentation

7:30 Discussion

- Governance Plan – HB 1612
- Revenue and Expense Update
- Board Goals Update
- SAU Building renovations/Capital Improvement Projects

7:50 Deliberations

- To see what action the Board will take regarding the proposed charter for the feasibility study for the SAU offices and barn as well as other HSTEP and capital improvement items identified by the committee
- To see what action the Board will take regarding the approval of the Governance Plan for HB 1612
- To see what action the Board will take regarding the policy memo submitted by the policy committee
- To see what action the Board will take regarding the administrations recommendation regarding the maintenance trust
- To see what action the Board will take to authorize the Superintendent to hire, accept resignations, and terminate staff during the summer months

8:10 Non – Public under RSA 91-A: 3II (a) Compensation and/or (c) reputation

8:20 Motion to adjourn

Hollis School District
Administrative Report
May 2019

Calendar, Events, Programs

- 6/6 and 6/7 - HPS 3rd Grade Concert at 1:45 pm
- 6/7 - HUES Field Day
- 6/11 - HUES Gr 6 students visit HBMS
- 6/12 - HPS Gr 3 students visit HUES
- 6/12 - HUES Gr 6 BBQ
- 6/12 - HUES Gr 4 Band Concert - 7pm
- 6/13 - HUES Gr 5 celebration of learning
- 6/14 - HUES Gr 6 celebration of learning
- 6/14 - HPS Field Day (Rain date 6/17)
- 6/18 - HUES Gr 6 Promotion Ceremony - 9:30am
- 6/19 - HPS/HUES - Step Up Day and Last Day dismissal (½ day)

Enrollment for 2018/2019:

HPS		**HUES**	
Grade	**Enrollment**	**Grade**	**Enrollment**
PreK 3	10	4	95
PreK 4	13 (+1)	5	100
K	80	6	123
1	76 (+1)		
2	83 (+1)		
3	93 (-1)		
Total Hollis School District Enrollment: 673			

Building & Grounds:

- HUES:
  - HUES has submitted a grant to the NRA School Shield Grant Program asking for $37K to help us reach more of our safety goals.
  - Details about summer work will be included in our end of year presentation.
- HPS:
  - Year end activities set-ups and breakdowns are the focus as we head into the end of the year
  - Details about summer work will be included in our end of year presentation
  - RTI and ESY summer classes will be held at HPS this summer. We are planning for additional cleaning and organizing to support student learning over the summer.

- A team of safety committee members are attending the Safety Preparedness Workshop to help us advance our safety goals.

Staffing & Students:

- HPS - Students from Mr. Ashley's class hosted this month's all school town meeting with a focus on Memorial Day. Students learned the difference between Memorial and Veterans Day.
- HPS - 3rd grade students finished their SAS assessments, all students worked hard and did a great job!
- HUES - Gr 4 will host families at their celebration of learning on 6/3
- HPS/HUES - Thank you to all our families and students as well as the PTA for making Teacher Appreciation Week so special for our staff members
- HUES celebrated another successful month with WING AWARDS for our students - we are so proud of their efforts in taking responsibility for their behavior, creating a climate of caring in the building.
- HUES staff and students hosted a Memorial Day Remembrance ceremony with a special recounting of the history of the Star Spangled Banner, a solo from Mr. Parent, and songs performed by our band students. We were very thankful to have our Veterans make time to participate in honoring our fallen soldiers with us.

Hollis School District
Monthly Enrollment Breakout
April 2019

Grade	Class size Per District Policy	Number of classes	NESDEC Projections 18/19 SY	Number of students (5/28/19)	Change from last report	Actual class Enrollments
Pre – K 3 year olds		1		10	0	10
Pre – K 4 year olds		1	18	13	+1	23
Kindergarten	18	5	80	80	0	15, 15, 16, 17, 17
Grade 1	18	5	71	76	+1	15, 15, 15, 15, 16
Grade 2	20	5	80	83	+2	16, 16, 17, 17, 17
Grade 3	20	5	94	93	-1	18, 18, 19, 19, 19
HPS Totals		**22 classes**	**325**	**355**		
Grade 4	23	5	96	95	0	19, 19, 19, 19, 19
Grade 5	23	5	107	100	0	18, 20, 20, 20, 22
Grade 6	23	6	125	123	0	20, 20, 20, 21, 21, 21
HUES Totals		**16 classes**	**328**	**318**		
HSD Totals		**38 classes**	**653**	**673**		

* denotes class sizes over policy expectations

Enrollment History:

School Year	HPS September Starting Enrollment Numbers	HUES September Starting Enrollment Numbers
2018	344	327
2017	344	323
2016	337	319
2015	345	295
2014	352	291
2013	358	292
2012	340	294
2011	340	297

Hollis School District

School Board Meeting:
June 5, 2019

District Goals
2018-2019

Presentation Overview

- 19/20 Staff
- Internal staff moves
- Mission/Vision Statement
- 2018-2019 Reflection on Goals
- Grade Level Configurations / Class Sizes SY 19/20
- Summer Work
- Looking Ahead

Hollis New Staff & Internal Staff Moves!

HPS:__

- Kindergarten (possible 5th)
- Environmental Science
- Nancy Kring Burns, Special Education Reading Specialist
- Brittany Ducharme, Case Manager
- Open Support Staff Positions

HUES:

- Sue Caron, Grade 4
- Paula Grieb, Specialist HUES
- Open Case Manager Position
- Open Support Staff positions

Hollis School District:
Every child, every day

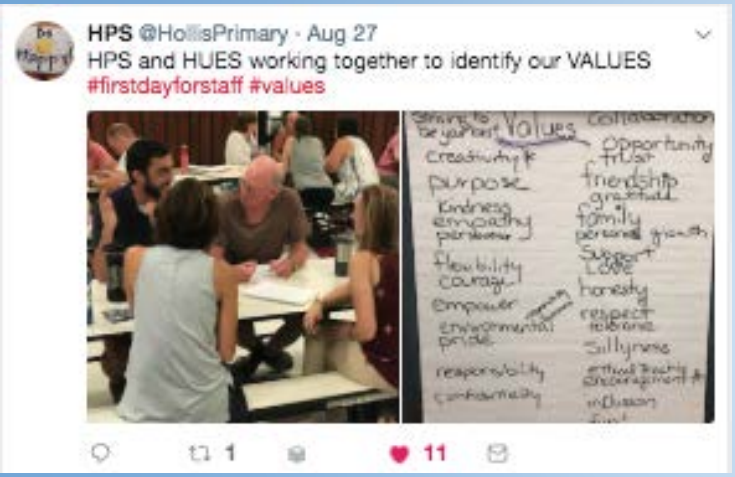
Mission

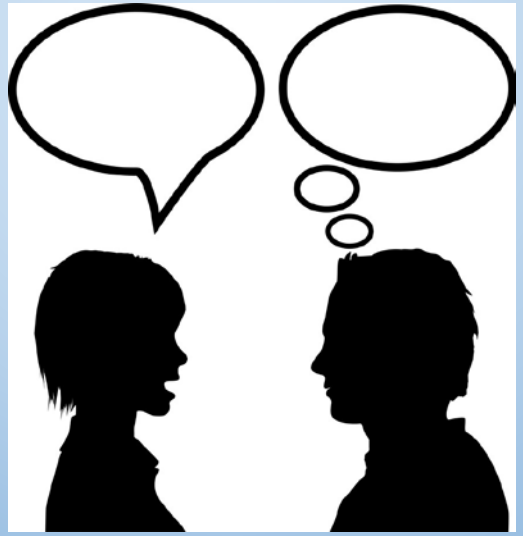
Consistent with the mission of SAU 41, we will ensure a strong, supportive learning environment focused on academic excellence.

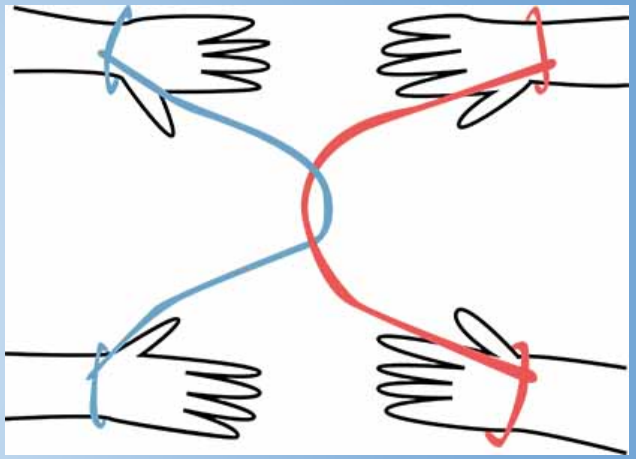
Vision Statement

The vision of Hollis School District staff is to work collaboratively to ensure, encourage, nurture, advance, promote, stimulate academic growth and develop a passion for community, learning and the life skills for: (1) independent learning, (2) social, and (3) emotional success in students.

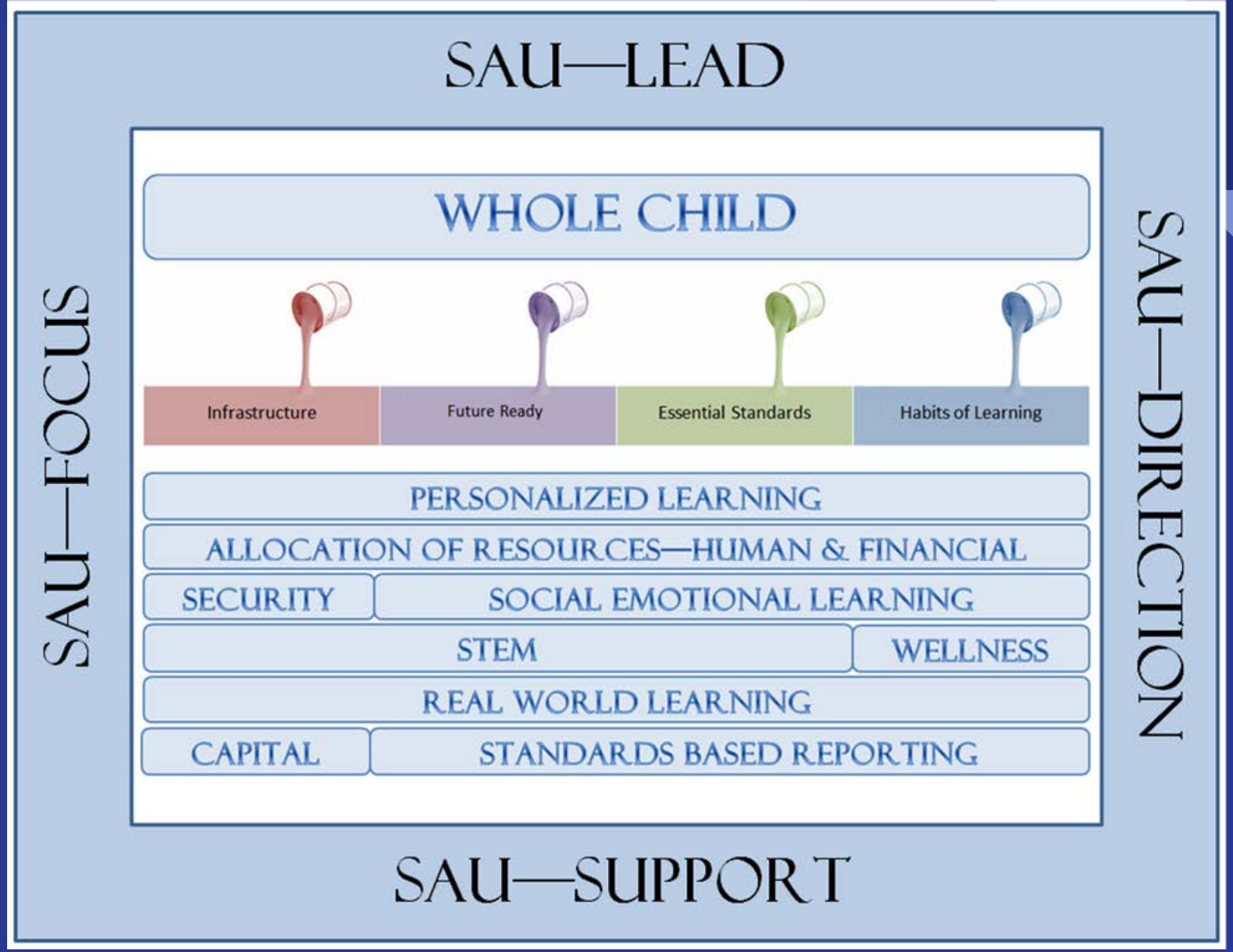
Hollis Theme for 2018-2019:



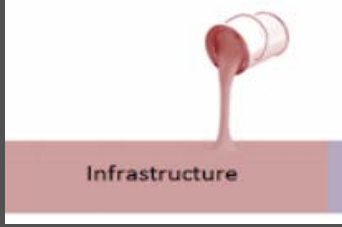




Role of SAU


SAU—LEAD
WHOLE CHILD
Infrastructure
Future Ready
Essential Standards
Habits of Learning
PERSONALIZED LEARNING
ALLOCATION OF RESOURCES—HUMAN & FINANCIAL
SECURITY
SOCIAL EMOTIONAL LEARNING
STEM
WELLNESS
REAL WORLD LEARNING
CAPITAL
STANDARDS BASED REPORTING
SAU—FOCUS
SAU—DIRECTION
SAU—SUPPORT

Infrastructure Goal:



Goal #1: Infrastructure (Safety/Security): Hollis School District will collaborate with emergency services and the SAU Joint Loss Management Committee (JLMC) to improve the safety and security of our schools.

Actions:

- **Emergency Operations Plans:** updated and submitted on time.
- **Grants and Budgetary Items:** HUES waiting to hear $37,000, HPS “fish bowl”, looking into more
- **Monthly Safety Committee Meetings**
- **Safety and Security Audits:** HPS DOE walkthrough, camera alignment, shades, flooring, HUES playground fencing, walkies for staff, additional cameras and bollards
- **Increase FEMA certified staff:** BOY - 29%
  HUES 53%
  HPS 40%
- **Collaboration with Police and Fire Departments:** Fire extinguisher training, Reunification, DARE, Lunches with an Officer

Social/Emotional Goal:

Goal #2: Habits of Learning (Social/Emotional): Continue building and embedding social/emotional programming that will continue to focus on developing students abilities to be: problem-solvers, resilient, independent, tolerant, as well as to be able to persevere through difficulty/failure, have an optimistic view and to have a growth mindset as learners.

- SEL TEAM MEMBERSHIP HUES & HPS
- HUES- SEL at faculty meetings
- HPS- SEL end of year training by members of the SEL Committee
- SEL TEAM- where we are heading
- Self-awareness, self-management
- Continued work on Tier 2 & 3

Academic Goal:

Academic Goal: Provide **staff** opportunities to build their depth of knowledge around standards, best practices and emerging trends in education.

Actions:

- Professional Staff will participate in Meaningful Monday work across districts
- Professional Staff will meet in PLC's to discuss, develop, refine, and share best practices to meet the needs of all learners
- Offer refined and differentiated professional development for the staff
- Continue with learning walks and classroom collaboration opportunities

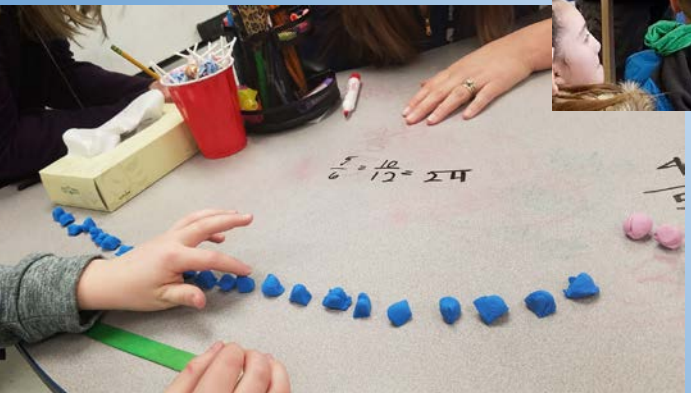
Academic Goal

Habits of Learning

Academic Goal: Create learning environments that are differentiated with opportunities that empower students to grow and reflect.

Actions:

- Continue to implement project based learning activities
- Foster student leadership via SOAR & town meetings
- Develop a consistent processes for gathering and using feedback from families and students
- Research and implement best practices for personalizing learning
- Refine RTI practices to include ALL learners
- Cultivate Talent




HELP OUT
STAY FIT
8
6
Respect Yourself
Respect Others
Respect Property
2


COMMUNICATION
COLLABORATION
exchange
Bumper Sensor
EVERY
SINGLE

Current Enrollment

School Year	HPS September Starting Enrollment Numbers	HUES September Starting Enrollment Numbers
2018	344	327
2017	344	323
2016	337	319
2015	345	295
2014	352	291
2013	358	292
2012	340	294
2011	340	297

Special Education Updates

Move-ins & increasing significance of student need is affecting special education staffing needs & budget

New substantially separate program at HPS

Continued work on early identification and remediation

Adaptive PE at HPS

Facility and Security Summer Upgrades

HUES:

- Flooring - Lower level
- Roof Replacement
- Painting - Lower level
- Key fobs for all doors
- Wi-fi upgrades
- Hot water heater replacement - 1st floor

HPS:

- Flooring in Makerspace and Nurse’s office
- Carpet in Learning Commons
- Shade Installation
- Playground equipment fixed
- Painting

Looking Forward:

- **Staffing, Programs, Facility, and Safety:**
  - HPS - Growing the ES position - recycling, composting, solar panel data, snowshoeing, composting and recycling.
  - HPS/HUES: Envisions 2 Implementation
  - HPS/HUES: Lucy Calkins Writing
  - HPS/HUES: CIP's
  - HPS/HUES - Continue to provide opportunities for training staff on emergency and safety protocols
  - HUES: Library / STEM Assistant addition

Rock Band performance at Talent Show

SAU41

Data Governance Plan

April, 2019

Contents

Introduction

SAU41 is committed to protecting our students' and staffs' privacy through maintaining strong privacy and security protections. The privacy and security of this information is a significant responsibility, and we value the trust of our students, parents, and staff.

SAU41's Data Governance Plan includes information regarding the data governance team, data and information governance, applicable School Board policies, District procedures, as well as applicable appendices and referenced supplemental resources.

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

SAU41's Data Governance Plan shall be a living document. To make the document flexible, details are outlined in the appendices and referenced supplemental resources. This document and any future modifications to this document will be posted on the District's website.

Data Governance Team

SAU41's Data Governance Team consists of the following positions: Assistant Superintendent, Business Administrator, Network Administrator, and Database Manager. Members of the Data Governance Team will act as data stewards for all data under their direction. The Network Administrator and Database Manager will act as the Information Security Officers (ISOs), with assistance from members of the full Technology team. All members of the district administrative team will serve in an advisory capacity as needed.

Purpose

The School Board recognizes the value and importance of a wide range of technologies for a well-rounded education, enhancing the educational opportunities and achievement of students. SAU41 provides its faculty, staff, and administrative staff access to technology devices, software systems, network and Internet services to support research and education. All components of technology must be used in ways that are legal, respectful of the rights of others, and protective of juveniles and that promote the educational objectives of the SAU41 School District.

To that end, the district must collect, create and store confidential information. Accurately maintaining and protecting this data is important for efficient district operations, compliance with laws mandating confidentiality, and maintaining the trust of all district stakeholders. All persons who have access to district data are required to follow state and federal law, district policies and procedures, and other rules created to protect the information.

It is the policy of SAU41 that data or information in all its forms, written, electronic, or printed, is protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment, software, and practices used to process, store, and transmit data or information. All staff and authorized district contractors or agents using confidential information will strictly observe protections put into place by the district.

Scope

The data security policy, standards, processes, and procedures apply to all students and staff of the district, contractual third parties and agents of the district, and volunteers who have access to district data systems or data. This policy applies to all forms of SAU41 School District data and information, including but not limited to:

- Speech, spoken face to face, or communicated by phone or any current and future technologies.
- Hard copy data printed or written.
- Communications sent by post/courier, fax, electronic mail, text, chat and/or any form of social media.
- Data stored and/or processed by any electronic device, including servers, computers, tablets, mobile devices.
- Data stored on any type of internal, external, or removable media or cloud based services.
- The terms data and information are used separately, together, and interchangeably throughout the policy, the intent is the same.
- Any computer, laptop, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device may be referred to as systems, assets or resources.
- All involved systems and information are considered assets of SAU41 and shall be protected from misuse, unauthorized manipulation, and destruction.

Regulatory Compliance

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix B: Laws, Statutory, and Regulatory Security Requirements). SAU41 complies with or exceeds the NH Minimum Standards for Privacy and Security of Student and Employee Data and standards applicable to data governance are addressed throughout this Data Governance Plan. SAU41 complies with all other applicable regulatory acts including but not limited to the following:

- Children's Internet Protection Act (CIPA)
- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Protection of Pupil Rights Amendment (PPRA)
- Individuals with Disabilities in Education Act (IDEA)
- New Hampshire State RSA - Student and Teacher Information Protection and Privacy
    - NH RSA 189:65 Definitions
    - NH RSA 189:66 Data Inventory and Policies Publication
    - NH RSA 189:67 Limits on Disclosure of Information
    - NH 189:68 Student Privacy
    - NH RSA 189:68-a Student Online Personal Information
- New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data
- 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 SAU41's information including: staff, students, volunteers, and authorized district contractors or agents. All data users are to maintain compliance with School Board Policies and District administrative procedures, EHAB (Data Governance and Security), GBEF (Employee Use of District-Issued Computers, Devices and the Internet, formally GCSA), GBEF-R (Employee Computer/Device and Internet Responsible Use Rules, formally GCSA-R), JICL (Student Use of Computers, Devices and the Internet, formally EGA), JICL-R (Student Technology Responsible Use, formally EGA-R) and all policies, procedures, and resources as outlined within this Data Governance Plan and School Board Policy.

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

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

Staff who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined or terminated. Volunteers may be excluded from providing services to the district. The district will end business relationships with any contractor who fails to follow the law, district policies or procedures, or the confidentiality provisions of any contract. In addition, the district reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of a staff member's teaching certificate.

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

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

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

- Unauthorized disclosure of PII or Confidential Information.
- Sharing your user IDs or passwords with others (exception for authorized technology staff for the purpose of support)
- 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.

• The unauthorized copying of system files.

• Attempting to secure a higher level of privilege without authorization.

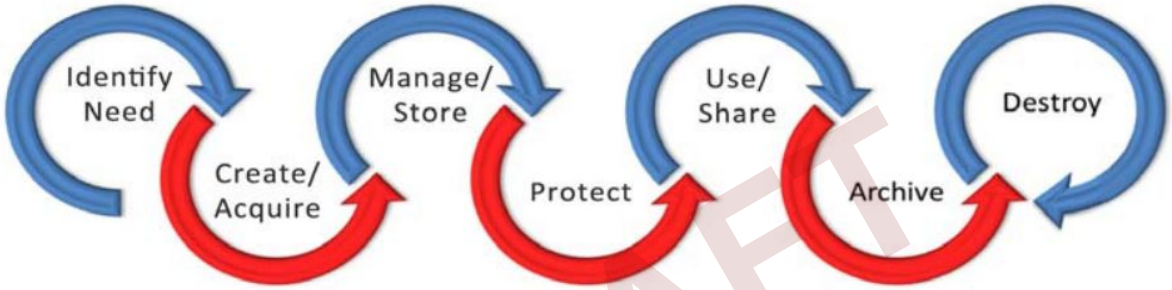
• Installation or use of unlicensed software or software not approved for district systems.

• The intentional unauthorized 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, security or video cameras, 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 district will collect, create or store confidential information only when the Superintendent or designee determines it is necessary.

New Systems

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

SAU41 has an established process for vetting new digital resources. Staff are required to complete steps outlined under the staff section of the SAU41's Technology Use and Student Privacy webpage, to ensure that all new resources meet business and/or instructional need as well as security requirements.

Memorandums of understanding (MOU), contracts, terms of use and privacy policy for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the Data Governance Team prior to initiation.

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

• Curricular value

- Technology environment impact, including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and ongoing costs
- Maintenance agreements, including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Terms of service, privacy policy, and MOU/contract that meet the following criteria:
    - o The district continues to own the data shared, and all data must be available to the district upon request.
    - o The vendor's access to and use of district data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.
    - o District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
    - o The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
    - o No API will be implemented without full consent of the Data Governance Team.
    - o All data will be treated in accordance to federal, state and local regulations.
    - o The provider assumes liability and provides appropriate notification in the event of a data breach.
    - Note: Exceptions can be made by the Data Governance Team when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent permission is requested from parents during the yearly online registration process for district vetted and approved applications and tools.

A current list of all vetted and approved software systems, tools and applications is published on SAU41s Technology Use and Student Privacy website.

Review of Existing Systems

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

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

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

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

Acquisition and Creation

After completing the requirements for adoption of any new systems, staff shall complete an online request form (located on the District's Staff Only Area) for any new digital app/tool that either has an associated cost or collects staff or student data (see Appendix C: Cloud/Technology Request Form). All staff must adhere to the following guidelines regarding a new digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the DGT prior to initiation.
- Prior to submitting the SAU41 Cloud/Technology Request Form, staff should speak with their building Technology Integrator or Administrator to evaluate to the site's content and use. No new app/online tool may be used until it has been vetted and approved by the DGT. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.
- It is the responsibility of the DGT to properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the Data Governance Team (DGT) prior to purchase.

Management and Storage

Systems Security

The district will provide access to confidential information to appropriately trained district staff and volunteers only when the district determines that such access is necessary for the performance of their duties. The district will disclose confidential information only to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law and authorized by the district (School Board Policy EHAB). Therefore, systems access will only be given on an as-needed basis as determined by the ISOs. Further information regarding Electronic Access Security Controls is contained in the Security/Protection section of this manual.

Data Management

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

Data Managers are responsible for the development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. All district administrators are data managers for all data collected and maintained of which they have been assigned to manage. Data managers will:

- ensure that system account creation procedures and data access guidelines appropriately match staff member job function with the data on instructional and operational systems.
- review all staff with custom data access beyond their typical group's access.
- review district processes to ensure that data will be tracked accurately.
- ensure that staff are trained in the district's proper procedures and practices in order to ensure

accuracy and security of data.

- assist the ISOs 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. 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 (ie. source document, electronic record, report) have the same classification regardless of format (see Appendix E: Data Classification Levels).

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

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

Security/Protection

Risk Management

A thorough risk analysis of all SAU41 School District's data networks, systems, policies, and procedures shall be conducted by an external third party or as requested by the Superintendent, ISOs or designee. An internal audit of District network security will be conducted annually by District Technology staff. This analysis shall be completed using the risk management steps outlined in the Data Security Checklist (Appendix D). 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.

Security Logs

The District 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 Network Administrator. In addition, access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals (see appendix G: Physical Security Controls).

No technological systems shall be disposed of or moved without adhering to the appropriate procedures (see Appendix H: Asset Management).

Inventory Management

The district shall maintain a process for inventory control in accordance to federal and state requirements and School Board policy. All district technology assets will be maintained in inventory and verified through the regular inventory verification process (see Appendix H: Asset Management).

Virus, Malware, Spyware, Phishing and SPAM Protection

The District uses a multi-layered approach to ensure that all electronic files are appropriately scanned for viruses, malware, spyware, phishing and SPAM. These include, but are not limited to, enterprise virus/malware/spyware software, group policy, gateways, firewalls, and content filter. Users shall not turn off or disable district protection systems or install other systems (see Appendix I: Virus, Malware, Spyware, Phishing and SPAM Protection).

Electronic Access Security Controls

District staff will only access personally identifiable and/or confidential information if necessary to perform their duties. The district will only disclose this information to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law. All staff are required to read and acknowledge applicable district policies as well as the SAU41 Acceptable Use Agreement, and sign documents annually.

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

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

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

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

Staff Users

All new staff accounts are authorized through an HR hiring process (see Appendix J: Account Management). Role-based permissions and security groups are used to establish access to all systems (see Appendix K: Data Access Roles and Permissions). If a staff member requires additional access, a request must be made directly

to the ISOs with a clear justification for access.

Contractors/Vendors

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

Password Security

The District will enforce secure passwords for all systems within their control (see Appendix L: Password Security).

Concurrent Sessions

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

Remote Access

Access into the District's network from outside is strictly prohibited without explicit authorization from the ISOs and Business Administrator. Remote access will be granted through the firewall from specific IPs to specific internal IPs; no other method of remote access shall be granted. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protection as information stored and accessed within District's network.

Securing Data at Rest and Transit

District data security applies to all forms of data, including data stored on devices, data in transit and data stored on additional resources. All district external hard drives will be maintained in inventory and verified through the regular inventory verification process. Regular transmission of student data to internal and external services is managed by the technology department using a secure data transfer protocol.

Users must ensure that they are securely storing their data. Guidelines have been established for Cloud Storage and File Sharing, External Storage Devices, and File Transmission Practices. (see Appendix F: Securing Data at Rest and Transit). These guidelines are outlined in the following section.

Usage and Dissemination

A consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. All district staff, volunteers, contractors and agents who are granted access to critical and confidential information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of confidential information. All individuals using confidential and critical information will strictly observe protections put into place by the district including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information in a confidential and secure manner.

All users are responsible for the security and integrity of the data they create, store or access. Users are expected to act as good stewards of data and treat data security and integrity with a high degree of responsibility and priority. Users must follow all guidelines outlined with Board policies, specifically Employee and Student Technology Usage (GBEF, GBEF-R, JICL, JICL-R), Data Governance and Security (EHAB),

and Student Records (JRA, JRA-R).

District staff, contractors and agents will notify the ISOs or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise.

Data Storage and Transmission

All staff and students that log into a district owned Macintosh and PC computers will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on the local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. Staff also will have a mapped personal folder. Access to these files is restricted to the folder's owner and district enterprise administrator accounts. Staff and students using Chromebook devices have limited local storage capabilities. Chromebook users are to store data within their G Suite for Education Drive account.

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with a Google G Suite for Education account that provides unlimited storage. Users are responsible for all digital content on their district provided Google G Suite for Education Drive (see Appendix F: Securing Data at Rest and Transit).

File Transmission Practices

Staff are responsible for securing sensitive data for transmission through email or other channels. Staff should not transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval. When possible, staff should de-identify or redact any PII or confidential information prior to transmission. Regular transmission of student data to services is managed by the technology department using a secure data transfer protocol (see Appendix F: Securing Data at Rest and Transit).

Credit Card and Electronic Payment

Users of systems that process electronic payments, including but not limited to processing credit card information, must adhere to strict guidelines regarding the protection of payment information and cardholder data. These users are responsible for adhering to the appropriate level of PCI compliance when handling such data (see Appendix F: Securing Data at Rest and Transit).

Mass Data Transfers

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

Printing

When possible, staff should de-identify or redact any PII or confidential information prior to printing. PII and confidential information shall not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

Oral Communications

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

Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or public areas.

Training

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

- Training for all staff on technology policies and procedures, including confidentiality and data privacy.
- Additional training for new instructional staff on federal regulations and the use of digital resources and student electronic records.
- Training for all instructional staff on federal regulations and the use of digital resources and student electronic records.
- Training for district administration on federal regulations, data privacy and security.
- All training or professional learning that includes the use of data systems shall include data security.

Archival and Destruction

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

District Data Destruction Processes

The district will regularly review all existing data stored on district provided storage for the purposes of ensuring data identification and appropriate destruction. Data destruction processes will align with School Board Policy EHB and EHB-R. District 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 G Suite for Education account will be suspended after the final day of enrollment and maintained for one school year after the student's final date of attendance.
- Staff G Suite for Education accounts will be suspended after the final work day, unless HR or the ISOs approves a district administrator to maintain access.

Asset Disposal

The district will maintain a process for physical asset disposal in accordance with School Board Policy DN. 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 (see Appendix H: Asset Management).

Critical Incident Response

Controls shall ensure that the District can recover from any damage to or breach of critical systems, data, or information within a reasonable period of time. Each school, department, or individual is required to report any instances immediately to the ISO or designee for response to a system emergency or other occurrence (for example, fire, vandalism, system failure, data breach and natural disaster) that damages/breaches data or systems.

Business Continuity

The District's administrative procedure EHB-R, delineates the timeline for data retention for all district data. The District 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 District's Technology Disaster Recovery Plan outlines critical staff, responsibilities, and processes in the event of a disaster or critical data loss. The District shall maintain a list of all critical systems and data, including contact information. The Technology Disaster Recovery Plan shall include processes that enable the District to continue operations and efficiently restore any loss of data in the event of fire, vandalism, natural disaster, or critical system failure (see Appendix M: Disaster Recovery Plan).

Data Breach Response

New Hampshire's data breach law (RSA 359-c:19, 20, 21) is triggered when a School District computer system is breached and personal information is acquired without authorization in a way that compromises the security or confidentiality of the information. The law requires a school district experiencing a breach to conduct a good faith and reasonably prompt investigation to determine the likelihood that personal information was, or will be, misused. The Data Breach Response Plan enables the District to respond effectively and efficiently to a data breach involving personally identifiable information (PII) as defined by NH Law, confidential or protected information (i.e. FERPA), district identifiable information and other significant cybersecurity incident. The Data Breach Response Plan shall include processes to validate and contain the security breach, analyze the breach to determine scope and composition, minimize impact to the users, and provide notification (see Appendix N: Data Breach Response Plan).

Appendix A - Definitions

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

Confidential Data/Information: Information that the district is prohibited by law, policy or contract from disclosing or that the district may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information (PII) regarding students and staff.

Critical Data/Information: Information that is determined to be essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Critical data is not necessarily confidential.

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

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

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

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

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

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

Information Security Officer: The Information Security Officers (ISOs) are responsible for working with the Superintendent, Data Governance Team, data managers, data owners, and users to develop and implement prudent security policies, procedures, and controls. The ISOs will oversee all security audits and will act as an advisor to:

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

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

Security Incident: An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2)

constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

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

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

User: The user is any person who has been authorized to read, enter, print or update information. A user of data is expected to:

- access information only in support of their authorized job responsibilities.
- comply with all data security procedures and guidelines.
- keep personal authentication confidential (user IDs, passwords, secure cards, PINs, access codes).
- report promptly to the ISOs 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/SAU41i/359-c/359-c-19.htm) Notice of Security Breach - Definitions
- NH RSA 359-C:20 (http://www.gencourt.state.nh.us/rsa/html/SAU41i/359-c/359-c-20.htm) Notice of Security Breach Required
- NH RSA 359-C:21 (http://www.gencourt.state.nh.us/rsa/html/SAU41i/359-c/359-c-21.htm) Notice of Security Breach Violation

Appendix C - Digital Resource Acquisition and Use

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

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

New Resource Acquisition

Staff are required to complete steps outlined under the District's Staff Technology page on the SAU41 website. An online cloud/website tool request form is required for any new digital resources to be used in the classroom. 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 Data Governance Team prior to initiation. Staff should speak with their building Technology Integrator before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be accessing content and/or any site that requires any student login.
- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the Data Governance Team.

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
- Terms of service, privacy policy, and MOU/contract that meet the following criteria:
    - o The district continues to own the data shared, and all data must be available to the district upon request.
    - o The vendor's access to and use of district data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.
    - o District data will be maintained in a secure manner by applying appropriate technical, B3 physical and administrative safeguards to protect the data.
    - o The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
    - o No API will be implemented without full consent of the district.
    - o All data will be treated in accordance to federal, state and local regulations

o The provider assumes liability and provides appropriate notification in the event of a data breach.

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

Approved Digital Resources

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

- A list of vetted software will be maintained on the SAU41 Software List on the District website.
- It is the responsibility of staff to submit a request to use a new digital resource if a resource is not listed.
- Digital resources that are denied or have not yet been vetted will not be allowed on district owned devices or used as part of district business or instructional practices.

Digital Resource Licensing/Use

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

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

- Only approved district resources are to be used.
- District software licenses will be:
    - kept on file at the District 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 SAU41 School District systems and other electronic devices will have a current license on file or will be removed from the system or device.
- Resources with or without physical media (e.g. downloaded from the Internet, apps, or online) shall still be properly vetted and licensed, if necessary, and is applicable to this procedure.
- Under no circumstances can staff act as a parental agent when creating student accounts for online resources; resources requiring this permission must be approved at the district level.

Appendix D - Data Security Checklist

A thorough risk analysis of all SAU41 School District data networks, systems, policies, and procedures shall be conducted as requested by the Superintendent, ISO or designee by an independent third party. The risk analysis will include internal and external vulnerability cybersecurity risk assessments and external penetration testing of the District network. An internal audit of District network security will be conducted annually by District Technology staff.

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

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

Data Security Checklist for District Hosted Systems

☐ Inventory and classification of data on system

☐ Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)

☐ Physical security of system

☐ Location within network including network systems protection (firewall, content filter) and if system is externally facing or only allows for district network access

☐ Access controls including password security (can district password requirements be enforced)

☐ Authentication methods (LDAP/Active Directory, Single Sign On, District managed account, user managed account)

☐ Server/system security patch frequency

☐ Ability to access from mobile devices

☐ Ability to maintain critical system event logs

☐ Ability to receive notification for critical system events

Data Security Checklist for Provider Hosted Systems

☐ Inventory and classification of data on system

☐ Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)

☐ Contract, terms of service and privacy policy are current and meet district data security requirements

☐ Provider has adequate data security measures including data management and incident response

☐ Ability to ensure proper access controls including password security (ie- can district password requirements be enforced)

☐ Authentication methods (LDAP/Active Directory, Single Sign On, District managed account, user managed account)

☐ Server/system security patch frequency

☐ Ability to access from mobile devices

☐ Notification practices in the event of a system compromise or security breach

Appendix E - Data Classification Levels

Personally Identifiable Information (PII)

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

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

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

Confidential Information

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

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

Internal Information

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

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

Directory Information

Directory Information is information contained in an education record of a student that generally would not be considered harmful or an invasion of privacy if disclosed without the consent of a parent or eligible student. SAU41 designates the following items as directory information:

- Student's name
- Address
- Parent Name and email address
- Telephone listing
- Participation and grade level of students in recognized activities and sports
- Height and weight of student athletes
- Years of attendance in the school district
- Honors and awards received
- Videos and photographs of student participation in school activities open to the public

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

Public Information

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

This information may be disclosed outside of the district.

Appendix F - Securing Data at Rest and Transit

All staff and students that log into a district owned Macintosh or PC computer will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on the local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. 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 a G Suite for Education account that provides unlimited storage. Users are responsible for all digital content on their district provided G Suite for Education Drive. 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 on Android & iOS. This will ensure that native operating systems do not replace cloud sharing security.
- Users need to be aware of default sharing settings on folders when they upload files. Users are required to limit sharing files to an as needed basis.
- Staff and students must ensure that any cloud storage providers used are approved by the district and meet district student data and data security standards.
- When exiting the district, students should responsibly copy their content to their own personal storage solution.
- When exiting the district, staff should ensure that they are only copying personal content that they created. Staff are prohibited from copying content that contains confidential information, student records or data.
- Data with personally identifiable information of staff or students may be posted to users' district provided Google Drive with appropriate security settings. Users may not post this data to other cloud sharing platforms without consent of district administration.
- Staff should never post any documents labeled classified, confidential, or restricted to any cloud storage including district provided Google Drive accounts without district approval.
- All users shall immediately report any cloud storage security problems of the district's technology resources to a teacher or administrator.
- Attempting to gain or gaining unauthorized access to cloud storage or the files of another is prohibited.
- As with other forms of district technology, district staff, students, and other G Suite for Education drive users have no expectation of privacy on data stored on this platform.

The term "File Sharing" is used to define all activities that share access to digital information whether in the cloud or on district administered mapped drives. When file sharing, staff must adhere to the following guidelines:

- Users must abide by all policies and procedures regarding professional conduct and communication when sharing, reviewing, updating, commenting and re-sharing.
- When sharing content, users must ensure that other users accessing the information in the files have appropriate access to the information based on job function.
- All users shall immediately report any inappropriate sharing of the district's technology resources to an administrator.

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 G Suite for Education Drive account for all storage needs. When using external storage devices, staff must adhere to the following guidelines:

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

File Transmission Practices

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

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.

Appendix G - Physical Security Controls RRTask

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 I: Asset Management).

Appendix H - Asset Management

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

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

Inventory

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

Disposal Guidelines

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

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

The Network Administrator shall approve disposals of any district technology asset.

Methods of Disposal

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

Discard

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

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

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

Donation/Gift

In the event that the district determines that an asset shall be donated or gifted, systems shall be wiped clean of Personally Identifiable Information (PII), Confidential, and/or Internal Information prior to leaving the school district. SAU41 will not support or repair any equipment that is donated. In addition, software licenses are not transferred outside the district. Therefore, systems must be returned to factory installation prior to donation.

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

SAU41 School District PC desktops, laptops, and file servers are protected using enterprise virus/malware/spyware software. Definitions are updated daily and an on-access scan is performed on all "read" files continuously. A full scheduled scan runs weekly. A full scheduled scan is performed on all servers weekly during non-peak hours. All files and systems are scanned.

Internet Filtering

Student learning using online content and social collaboration continues to increase. SAU41 views Internet filtering as a way to balance safety with learning, letting good content, resources, and connections in while blocking the bad. To balance educational Internet resource and application use with student safety and network security, the Internet traffic from all devices on the district network is routed through the district firewall and content filter. Filtering levels are based on the role of the user, staff or student and student grade level. All sites that are known for malicious software, phishing, spyware, etc. are blocked.

Phishing and SPAM Protection

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

Security Patches

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

Appendix J - Account Management

Access controls are essential for data security and integrity. SAU41 maintains a strict process for the creation and termination of district accounts. All new staff accounts are authorized through an HR hiring process prior to creation. Role-based permissions are used to establish access to all systems. Access security is audited at least annually or whenever access permission requirements are changed for a particular application/software or when an application/software is no longer necessary.

Staff Accounts

When a staff member is hired by SAU41, the following process ensures that each staff member has the correct access and permissions to the resources that are required for their position.

- Notification of new staff member is sent from Human Resources to the Technology Department. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology Department creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s) (see Appendix K: Data Access Roles and Permissions).
- Any exception to permissions must be approved by the district administrator responsible for the system (Database Manager and the Network Administrator.

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

- In the event of termination, HR will notify the Technology Department via email or phone call requiring the account to be disabled at once, preventing any further access to district resources.
- In the event of resignation, HR will notify the Technology Department via email indicating the termination date. The account is disabled at the end of business on the termination date, preventing further access to district resources.
- In the event that a user having elevated permissions to any system separates from the district, additional measures are taken to ensure that all elevated accounts to those systems are secure.

Local/Domain Administrator Access

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

Remote Access

Access into the District's network from outside is strictly prohibited without explicit authorization from the ISOs. PII, confidential information and/or Internal Information that is stored or accessed remotely shall maintain the same level of protection as information stored and accessed within District's network.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by HR and ISOs. and must follow District security protocols for contractors and vendors. All contractors/vendors accessing district data will be considered on premise users.

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

Staff are entered into SAU41's student information system. Only staff whose roles require access are provided accounts for the system. The following minimum information is entered for each staff member:

- Building/site location
- Status - active
- Staff type/position
- District email address
- Primary Alert phone number and mobile phone number

Access accounts for the District's SIS are setup based on staff role/position, building and required access to student data and are assigned by the Database 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. 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
- Athletic
- Counselor
- IT Staff
- Office Staff
- Principal
- Registrar
- Nurse
- Secretary II
- Super Amin
- Unassigned - no access

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

Financial System

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

- Accounting Specialist
- Administrator
- Full Access
- HR
- Read Only
- Maintenance
- Spec Ed Coordinator
- Spec Ed Secretary
- Sr. Secretary

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

Special Education System

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

- Case Manager
- District Administrator
- District IT Administrator
- General Ed Teacher
- IEP Team Member
- SAU Authorized Official
- SAU District Administrator
- SAU System Administrator
- School Administrator

Health Software System

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

Food Services System

The District uses a Food Services software management system to track data and perform functions necessary for the efficient 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. The established roles are as follows:

Security Roles

Web Roles	Register Roles
• Administrator	• Administrators
• Manager	• POS Cashier
	• Manager

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

Appendix L - Password Security

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

- Passwords shall never be shared with another person.
- When possible, user created passwords should adhere to the same criteria as required for district network access as outlined below.
- Passwords shall never be saved when prompted by any application systems as approved by the Technology Department.
- Passwords shall not be programmed into a computer 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 staff who have reason to believe a password is lost or compromised must notify the Director of Technology or designee as soon as possible. The technology department will verify the identity of the person requesting the change before resetting the password.

District network access to resources managed through LDAP

- Passwords must be "strong," and must be a minimum of 8 characters long, must include at least one uppercase character, one number and one special character (! @ # $ % & ?)
- Passwords will be changed every 90 days or sooner, if the user believes the log on credentials have been compromised.
- Your password must not be too similar to your username.
- Do not use your district password for any non-district systems.

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

- Passwords routed over a network shall be encrypted.
- Passwords shall be entered in a non-display field.
- System software shall enforce the changing of passwords and the minimum length.
- System software shall disable the user password when more than five consecutive invalid passwords are given.

Appendix M - Technology Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable SAU41 (SAU41) 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 SAU41's 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 utilize existing storage to recover systems.
- District data is housed at district data centers and backed up in the cloud.
- District data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

The SAU41 has appointed the following people to the disaster recovery/critical failure team: Network Administrator, Assistant Superintendent, Database Manager, and Business Administrator.

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

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

Activation

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

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

The Information Security Officers (ISOs) will act as the incident response managers (IRMs). If the ISOs are not able to act as the IRMs, a member of the Superintendent's Leadership Team will assume the role of IRM, with assistance from the Incident Response Team (IRT).

Notification

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

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

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

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

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

Implementation

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

- Maintained spreadsheet listing all server names, physical and virtual, and their function. An electronic version will be housed on Google Drive.
- Maintained secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.
- The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and the cloud. The District's critical virtual servers are backed up to an image file.
- In the event of a critical system failure, the District can restore that server back to our current environment from the backup solution.

Deactivation

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

Evaluation

An internal evaluation of the SAU41's TDRP response will be conducted. This will entail gathering documentation from the response and feedback from all stakeholders and incorporate into an after action report and corrective action plan. The result will be an update to the TDRP and other emergency response plans as appropriate.

Appendix N - Data Breach Response Plan

Objectives

The purpose of the Technology Data Breach Plan (TDBP) is to enable SAU41 (SAU41) 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 SAU41's TDBP:

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

Data Breach/Incident Response Team

SAU41 has appointed the following people to the data breach/incident response team: Network Administrator, Assistant Superintendent, Database Manager, and Business Administrator.

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

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

Activation

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

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

The Information Security Officers (ISOs) will act as the incident response managers (IRMs). If the ISOs are not able to act as the IRMs, the Assistant Superintendent will assume the role of IRM, with assistance from the IRT. The breach response and reporting process will be documented according to state and federal requirements. The Network Administrator will work with the Superintendent to dispense and coordinate the notification and public message of the breach.

Notification

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

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

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

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

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

Implementation

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

• Data inventory of all systems containing sensitive data. A hard copy of this document will be secured at the technology office. An electronic version will be housed on the Technology Departments Team Drive.

• Data dictionary of all district hosted information systems. A hard copy of this document will be secured at the technology office. Due to non-disclosure agreements, this data may not be available in other locations/formats. The appropriate vendor(s) can be contacted for this information.

• Maintained spreadsheet listing all server names, physical and virtual, and their function. An electronic version will be housed on the Technology Information Team Drive.

• Maintained secure document to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.

• The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and offsite.

The following will take place during the incident response:

• The members of the IRT will be assembled once a breach has been validated. The IRT will be comprised of the Network Administrator, Database Manager, Assistant Superintendent, Business Administrator. Additional members of SAU41's administrative team and technology department may be designated to assist on the IRT.

• The IRT will determine the status of the breach, on-going, active, or post-breach. For an active and ongoing breach, the IRT will initiate appropriate measures to prevent further data loss. These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.

• The IRT will work with the data managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.

• The IRMs will work with legal counsel and the Superintendent's Leadership Team to determine appropriate course of action pursuant to state statute. This includes notification of the authorities, and local law enforcement.

• Collaboration between the authorities and the IRT will take place with the IRMs. The IRT will work with the proper authorities to make sure any and all evidence is properly handled and preserved.

• On advice from legal counsel, an outside party may be hired to conduct the forensic investigation of the breach. When the investigation has concluded, all evidence will be safely stored, recorded or destroyed (where appropriate).

• All affected data, machines and devices will be identified and removed from the network as deemed appropriate for the investigation. Interviews will be conducted with key personnel and facts of the incident will be documented and the evidence preserved for later examination.

• The IRT will work with the Superintendent's office to outline the notification of the data owners and

those affected. Communication will be sent out as directed by legal counsel and advised by the data governance team. The types of communication will include, but not limited to, email, text message, postal mail, substitute notice and/or phone call.

• The IRMs, in conjunction with the IRT, legal counsel and the Superintendent's Leadership Team will determine if notification of affected individuals is necessary. Once the determination is made to notify affected individuals, a letter will be written in accordance with all federal and state statutes, and local procedures. If it is determined that identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and filed at the Superintendent's office.

Deactivation

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

Evaluation

Once the breach has been mitigated an internal evaluation of the SAU41's TDBP response will be conducted. The IRT, in conjunction with the IRMs and others that were involved, will review the breach and all mitigation steps to determine the probable cause(s) and minimize the risk of a future occurrence. Feedback from the responders and affected entities may result in an update to the TDBP and other emergency response plans as appropriate. Information security training programs will be modified to include countermeasures to mitigate and remediate previous breaches so that past breaches do not recur. The reports and incident review will be filed with all evidence of the breach.

STATUS REPORT: SAU41 & SB1612

TECHNOLOGY TEAM: RICHARD RAYMOND, KELLY SEELEY, CAROL TYLER, GINA BERGSKAUG

HB 1612 Signed by Governor Sununu June 18, 2018

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1 New Paragraph; Student and Teacher Information Protection; Data Inventory Security Plan. Amend RSA 189:66 by inserting after paragraph IV the following new paragraph:

V. The department shall establish minimum standards for privacy and security of student and employee data, based on best practices, for local education agencies. Each local education agency shall develop a data and privacy governance plan which shall be presented to the school board for review and approval by June 30, 2019. The plan shall be updated annually and presented to the school board. The plan shall include:

(a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use.

(b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed standards set by the department.

(c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools and extensions.

(d) A response plan for any breach of information.

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

2 Student and Teacher Information Protection; Data Inventory Security Plan. Amend the introductory paragraph of RSA 189:66, IV to read as follows:

IV. The department ***and each local education agency*** shall make publicly available students' and parents' rights under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. section 1232g, et seq., and applicable state law including:

3 Effective Date. This act shall take effect 60 days after its passage.

SAU 41
HOLLISBROOKLINE

Prior to HB1612:

Data Security Framework was implemented

Assigned Roles

- created a list of roles-based security in software systems
- set permissions based on need

Updated the Acceptable Use Agreement (AUA)

- reviewed with new lens

Prepared a Software Inventory

- categorized and listed resources: licensed software, free tools/websites, curricular resources, chrome extensions, and paid library databases

SAU 41
HOLLISBROOKLINE

Per HB1612, inventoried, reviewed and vetted existing software applications

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1 New Paragraph; Student and Teacher Information Protection; Data Inventory Security Plan. Amend RSA 189:66 by inserting after paragraph IV the following new paragraph:

V. The department shall establish minimum standards for privacy and security of student and employee data, based on best practices, for local education agencies. Each local education agency shall develop a data and privacy governance plan which shall be presented to the school board for review and approval by June 30, 2019. The plan shall be updated annually and presented to the school board. The plan shall include:

(a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use.

(b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed standards set by the department.

(c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools and extensions.

(d) A response plan for any breach of information.

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

2 Student and Teacher Information Protection; Data Inventory Security Plan. Amend the introductory paragraph of RSA 189:66, IV to read as follows:

IV. The department ***and each local education agency*** shall make publicly available students' and parents' rights under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. section 1232g, et seq., and applicable state law including:

3 Effective Date. This act shall take effect 60 days after its passage.

SAU 41
HOLLISBROOKLINE

Compiled and distributed an inventory of all district software

Unlicensed **Software**

Used by Brookline	Used by Hollis	Used by COOP	Name of Service / Software	Description	Website	Privacy Statement	Terms of Use
K-3	3		sheppard software	games and resources	http://www.sheppardsoftware.com/	http://www.sheppardsoftware.com/privacy.htm	
K-6 teachers	3		BEtter Lesson	PD for teachers	https://betterlesson.com/	https://pd.betterlesson.com/privacy-policy/?from=bl_landing_footer	
K-3	4		Epic	Epic! provides an unlimited selection of eBooks that can be instantly discovered, read and shared with friends. Personalized for each individual reader,	https://www.getepic.com/sign-in	https://www.getepic.com/privacy	https://www.getepic.com/tos
1-3	1-6	9-12	Math Playground	Math Games	https://www.mathplayground.com/	https://www.mathplayground.com/privacy.html	
4-6	4-6	7-12	Read 180	Reading Comprehension Intervention Program	https://idp-awsprod1.education.scholastic.com/idp/	https://www.hmhco.com/privacy-policy-k12-learning-platforms	http://d5oojzteh1rf3.cloudfront.net/10/2b/f31acede40bb9af6f4deae68f70f/terms-pdf.pdf
n/a	4-6	9-12	Kahoot!	Assessment/Gaming tool	https://kahoot.it/#/	https://getkahoot.com/info/privacy-policy	https://getkahoot.com/info/terms-and-conditions
n/a	4-6	9-12	Project Lead The Way	Engineering course credit program	https://my.pltw.org/	https://www.pltw.org/privacy-policy	https://www.pltw.org/terms-of-service
RMMS teachers	4-6	10-11	Canvas	Infographic Website	https://www.canva.com/	https://about.canva.com/privacy-policy	https://about.canva.com/terms-of-use/
2-3	4-6	7-12	EasyBib Bibliography	Bibliography Tool	http://www.easybib.com/	http://www.easybib.com/company/privacy	http://www.easybib.com/company/terms
4-6	4-6	7-12	Google Maps	Web Mapping Service	http://maps.google.com	https://www.google.com/intl/en/policies/privacy/	https://www.google.com/intl/en/policies/terms/
	4-6	7-8	Quizlet	Assessment Tool	https://quizlet.com	https://quizlet.com/privacy	https://quizlet.com/tos
K-3	4-6		Plickers	Assessment tool	https://www.plickers.com/	https://plickers.com/privacy	https://www.plickers.com/terms
	4-6		Prodigy Math	Math Game	https://www.prodigygame.com/	https://www.prodigygame.com/privacy-policy/	https://www.prodigygame.com/terms-conditions/
	4-6		Bankaroo	Behavior management (HUES bucks, etc.)			
1-3	1 - 3		Typing Club	Online Typing Program	https://www.typingclub.com/	https://www.typingclub.com/privacy.html	https://www.typingclub.com/terms.html
K-3; 4-5	1 - 6	9-12	code.org	Computer Science Education	https://code.org/	https://code.org/privacy	https://code.org/tos

Information must be submitted

Implemented Software Security Guidelines

Began with those submitted

- Does it meet the privacy standard?
  - Require student log in, collect/tracking data, etc.
- Does it contribute to the curriculum?
  - Competing pop-ups, targeted marketing, enhance v. distraction
- Is there a cost both initial and/or on-going?

Required Cloud-Based Technology Use Request Form

- Vetted individual submissions
- Set permissions based on need

SAU 41
HOLLISBROOKLINE

Developed Protocols for Protection of Student Data

Some resources require logins

- How do we standardize student information that will be uploaded?
- Who uploads student information?
- When is explicit parental permission required?

How do we communicate our practices

- Data security
- Curricular Right-to-Know
- Annual PowerSchool Enrollment Software

SAU 41
HOLLISBROOKLINE

Conducted Mandatory Student Privacy and Data Security Trainings in June 2018

Training Included:

Cloud-Based Software Criteria

- Privacy pledge from vendor – who product is geared toward?
- 13+ guidelines
- Additional permission forms….when are they required?

Guidelines for Data Privacy and Security

The following are **NOT PERMITTED** unless the Cloud Software Form has been approved and returned to you by SAU41 Central Office

- Creating student accounts
- Creating student access to websites
- Adding student names for free trials
- Adding temporary tools

When approved, students will be uploaded or prepared for you according to the Cloud Tech guidelines

SAU 41
HOLLISBROOKLINE

SAU 41 Technology Initiative Approval Request
Cloud Based Software Services

Title of Cloud Vendor: _____
Author Contact Information: _____
School: _____
Desired Implementation Date: _____

Because student privacy and FERPA considerations are of the utmost importance, it is critical that information extracted from any SAU41 database for the purpose of uploading to any Internet cloud system be evaluated and approved by administration.

1. Description of cloud technology request.
What is the name of the cloud system. (include URL)
How did you hear about the site?
What and how will curriculum will be delivered?
Were other options considered?
Who will be using this site?
What type of information will students be entering?

2. Who will be using this technology (Administrators, Prof Staff, Support Staff, Office Staff, Students, Other? Please check all that apply.
Technology users: Check (X) all that apply:
Administrator __ Professional Staff ___ Support Staff __ Office Staff __ Students __ Other __

3. Does it require student information to be uploaded? Please be specific as to what student information will be uploaded. Place X next to all that apply.	
☐ PowerSchool ID -	☐ Date of Birth
☐ Last Name (powerschoolid) -	☐ Home Room
☐ First Name	☐ Password
☐ Grade Level	☐ Student Email
☐ School	☐ Other (Indicate the information)

4. FERPA Considerations
Does the site have any age restrictions? (some sites require guardian permission if a child is under 13 years of age)
Please include a link to the vendor's privacy statement.
Has the vendor signed the Student Privacy Pledge?
Have other schools in the area been contacted for their experience.

5. Funding?	
Is there a cost and is it budgeted?	
Account line for funding?	
What is the cost per user and total cost?	
If there is a recurring cost, what amount and how will the cost be funded?	

6. Professional Development: How will Professional Development for staff be delivered? If funding is needed for PD, how will it be funded?

7. Technology Department - Please discuss with Network Administrator as needed.
Will the current network bandwidth support the initiative? Will adjustments need to be made to the Internet filter or firewall? Will there be required Professional Development for the tech dept? How will the PD be funded and delivered?

8. Who will manage accounts and setup of the cloud service?
Will this initiative need ongoing support and maintenance (ie creating/deleting accounts/passwords)? If so, who do you see as the person(s) providing these functions? How will account maintenance be managed? (if a student or staff member leaves the district how will the account deletion be managed)

Technology Initiative Review Signatures: **MUST HAVE ALL SIGNATURES**

Staff Member: _____ Date: _____

Principal: _____ Date: _____

For SAU Office Use Only
Approval Request Process:
Date Received_____ Initials _____

Committee Meeting Date: _____
Approved: ☐ Yes ☐ No Date: _____
Reason if not approved: _____

Signatures once approved/disapproved:
Business Administrator_____ Date: _____

Network Administrator _____ Date: _____

Assistant Superintendent _____ Date: _____

Student Data

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1 New Paragraph; Student and Teacher Information Protection; Data Inventory Security Plan. Amend RSA 189:66 by inserting after paragraph IV the following new paragraph:

V. The department shall establish minimum standards for privacy and security of student and employee data, based on best practices, for local education agencies. Each local education agency shall develop a data and privacy governance plan which shall be presented to the school board for review and approval by June 30, 2019. The plan shall be updated annually and presented to the school board. The plan shall include:

(a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use.

(b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed standards set by the department.

(c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools and extensions.

(d) A response plan for any breach of information.

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

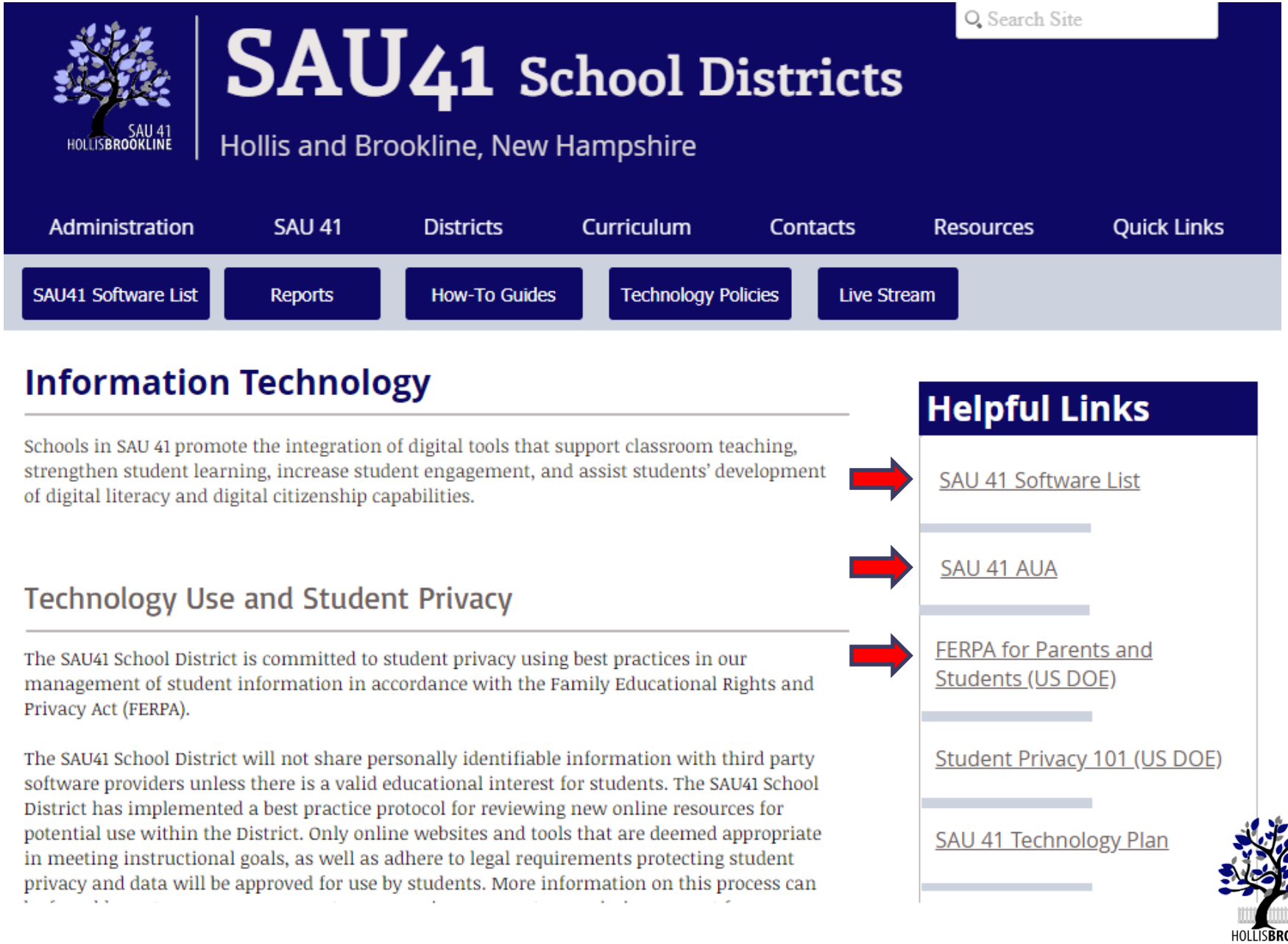
2 Student and Teacher Information Protection; Data Inventory Security Plan. Amend the introductory paragraph of RSA 189:66, IV to read as follows:

IV. The department ***and each local education agency*** shall make publicly available students' and parents' rights under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. section 1232g, et seq., and applicable state law including:

3 Effective Date. This act shall take effect 60 days after its passage.

SAU 41
HOLLISBROOKLINE

www.sau41.org


Search Site
SAU41 School Districts
Hollis and Brookline, New Hampshire
Administration
SAU 41
Districts
Curriculum
Contacts
Resources
Quick Links
SAU41 Software List
Reports
How-To Guides
Technology Policies
Live Stream
Information Technology
Schools in SAU 41 promote the integration of digital tools that support classroom teaching, strengthen student learning, increase student engagement, and assist students' development of digital literacy and digital citizenship capabilities.
Technology Use and Student Privacy
The SAU41 School District is committed to student privacy using best practices in our management of student information in accordance with the Family Educational Rights and Privacy Act (FERPA).
The SAU41 School District will not share personally identifiable information with third party software providers unless there is a valid educational interest for students. The SAU41 School District has implemented a best practice protocol for reviewing new online resources for potential use within the District. Only online websites and tools that are deemed appropriate in meeting instructional goals, as well as adhere to legal requirements protecting student privacy and data will be approved for use by students. More information on this process can
Helpful Links
SAU 41 Software List
SAU 41 AUA
FERPA for Parents and Students (US DOE)
Student Privacy 101 (US DOE)
SAU 41 Technology Plan

SAU 41 Software List

SAU41 Software

Used by Brookline	Used by Hollis	Used by COOP	Name of Service / Software	Description	Publisher Website	Privacy S
		7-12	Adobe Creative Suite	Software suite of graphic design, video editing, and web development applications	http://www.adobe.com	installed l
K-6	K-6	7-12	AESOP	Substitute and Absence Management System	https://www.aesoponline.com	http://www s/Privacy_
	K-6		AIMS Web	Benchmarking Assessment and Progress Monitoring tool	https://aimsweb.pearson.com/	
K-6	K-6	7-12	Alert Solutions	School Notification System	https://www.alertsolutions.com/	https://ww policy/
K-6	K-6	7-12	AppliTrack	Human Resource Employment Application System	http://www.applitrack.com/sau25/onlineapp/	http://www s/Privacy_
	K-6		Brain Pop/BrainPop Jr.	Online interactive curriculum content	https://www.brainpop.com/	https://ww _policy/
		9-12	Career Cruising	A self-exploration and planning program that helps people of all ages achieve their potential in school, career and life.	https://public.careercruising.com/en/	https://pub acy-policy
4-6	4-6		Defined Stem	Project-based learning solution that providing lessons built around careers.	www.definedstem.com	https://ww
K-6 CLICK HERE	K-6	7 CLICK HERE	Destiny	Library Automation and Resources	http://destiny.sau25.net	hosted int

Licensed Software | Free Tools/Websites | Curricular Resources | Chrome Extensions | Paid Library Databases

* Approved with expressed parent permission

SAU 41 HOLLISBROOKLINE

Data Governance Plan

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1 New Paragraph; Student and Teacher Information Protection; Data Inventory Security Plan. Amend RSA 189:66 by inserting after paragraph IV the following new paragraph:

. The department shall establish minimum standards for privacy and security of student and employee data, based on best practices, for local education agencies. Each local education agency shall develop a data and privacy governance plan which shall be presented to the school board for review and approval by June 30, 2019. The plan shall be updated annually and presented to the school board. The plan shall include:

(a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use.

(b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed standards set by the department.

(c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools and extensions.

(d) A response plan for any breach of information.

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

2 Student and Teacher Information Protection; Data Inventory Security Plan. Amend the introductory paragraph of RSA 189:66, IV to read as follows:

IV. The department ***and each local education agency*** shall make publicly available students' and parents' rights under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. section 1232g, et seq., and applicable state law including:

3 Effective Date. This act shall take effect 60 days after its passage.

Data Governance Plan Development

Data Governance Team

- Richard Raymond, Carol Tyler, Kelly Seeley, Gina Bergskaug
- Understand purpose and intent of DGP
- Develop the DGP

Define Data Lifecycle & Data Security

- Identify potential need, based on District Systems Assessment
- Perform Risk Assessment and External Audit for potential opportunities for breach
- Define data retention and destruction processes
  - Data at rest on recycled hardware
  - Data at rest on current and outdated database systems

SAU 41
HOLLISBROOKLINE

Data Governance Plan

Plan for Critical Incident Response

- Business continuity
- Data recovery
- External and internal response plan including communication

Policy Work

- EHAB
- GBEF
- GBEF-R
- JICL
- JICL-R

SAU 41
HOLLISBROOKLINE

Next Steps

Tackling the Requirements

- Complete a Network Audit
- Complete a Security Audit
- Identify funding source

Ongoing Work…

- Vetting new sites
- Reviewing existing “approved” sites for updates to privacy policy or terms of use
- Data retention and storage

SAU 41
HOLLISBROOKLINE

Hollis School District
Expense Revenue Report

Hollis **FY19**

THRU 05/29/19

Expense Function	Description	Annual Budget	YTD Expense	Encumbered	Balance	Reason
1100	**Regular Education**	3,977,924.99	2,938,867.48	968,214.37	70,843.14	*<Unfilled Para positions and Sub needs*
1200	**Special Education**	1,168,879.23	1,085,668.04	81,308.71	1,902.48	
2100	**Student Support Services**	897,144.27	631,996.03	167,893.61	97,254.63	*<Contracted Services for students less than expected*
2200	**Instructional Staff Support**	418,453.20	245,564.26	83,930.86	88,958.08	*<PD less than expected*
2300	**School Board/SAU Assessment**	625,014.00	487,746.21	43,687.87	93,579.92	*<Includes $95K Contingency, plus Negotiations legal fees higher*
2400	**School Administration**	625,629.49	563,404.11	73,066.62	(10,841.24)	*<Various small overages*
2600	**Facilities**	728,644.05	758,940.55	89,658.32	(119,954.82)	*<Utilities higher than expected (Propane/Electric)*
	Water System (10.2600.411)	17,500.00	10,620.97	1,847.97	5,031.06	
2700	**Transportation**	452,604.55	345,395.86	32,654.49	74,554.20	*<Gasoline less than expected and Bus route credits*
2900	**Benefits**	2,613,528.73	2,084,807.53	557,935.03	(29,213.83)	*<Healthcare plan shifts to more family plans*
4200/4300	**Building Improvements**	-	6,330.00		(6,330.00)	*<SAU Barn feasibility study*
5100	**Bonds**	324,387.49	324,387.49		-	
5200	**Transfers**	539,970.00	158,970.00	381,000.00	-	
		12,389,680.00	**9,642,698.53**	**2,481,197.85**	**265,783.62**	
	FY18 CarryOver	61,901.24	54,583.94	4,370.95	2,946.35	
		12,451,581.24	**9,697,282.47**	**2,485,568.80**	**268,729.97**	

Revenue		Budget	Revenue	Expected	Balance	
1100	**Local Property Tax**	9,079,409.00	8,133,621.00	945,788.00	-	
3110	**Adequacy Aid Grant/Tax**	2,433,340.00	2,433,340.00	-	-	
	State					
3220	Kindergarten Aid	70,903.00	70,902.81		0.19	
3230	Special Education Aid	2,213.00	2,774.90	-	(561.90)	
21.3260	Food Service	3,000.00	3,203.94	-	(203.94)	
	Federal					
22.4100-4539, 4570	Grants	60,000.00	9,261.58	50,738.42	-	
21.4560	Food Service	34,000.00	24,318.13	9,681.87	-	
	Disabilities Programs	110,000.00	-	110,000.00	-	
4580	Medicaid	46,000.00	26,707.96	5,000.00	14,292.04	
	Local					
1311, 1349	Tuition	20,000.00	25,189.56	4,575.64	(9,765.20)	*Increase in PreSchool kids & unexpected Non-Resident Tuition*
21.1600-1699	Food Service Sales	174,000.00	168,000.00	6,000.00	-	
1510, 1910, 1991	Other	22,000.00	34,688.62		(12,688.62)	*Worker's Comp - Premium Holiday*
	Voter Trusts (FY18)		-		-	
	Less Maintenance Trust	90,000.00	-	90,000.00	-	
	Less SAU Building Trust	18,970.00	-	18,970.00	-	
	Less Water System Exp Trust	50,000.00	-	50,000.00	-	
	Fund Balance to Reduce Taxes (FY 19)	327,845.00	-	327,845.00	-	
	Less Retained Funds (FY19)	(152,000.00)	-	(152,000.00)	-	
		12,389,680.00	**10,932,008.50**	**1,466,598.93**	**(8,927.43)**	

Unreserved Fund Balance		**277,657.40**	
FY20 Actuals			
Less SAU Building Trust	$	23,970	
Less Maintenance Trust	$	120,000	
Less SPED Trust	$	25,000	
Less Retained Fund Balance	$	132,657	*<Traditionally $152K - voted on in August*
Fund Balance to Reduce Taxes	**$**	**0**	

Hollis School District

Expendable Trust: Public Hearing

June 5, 2019

Hollis School Buildings Expendable Trust

Background

Principals Paula Izbicki and Candi Fowler identified several needed repairs/improvements for their respective buildings during the budget process. At the 2018 Budget Hearing, the Hollis Budget Committee recommended along with the Hollis School Board that the funding source for these particular items be the Hollis School Building Expendable Trust.

The Trust has also been suggested as the funding source for two additional items: the unexpected replacement of the heating control unit at HPS and the unexpected roof replacement under the solar panels at HUES (the amount not covered by the lease and the rebates).

FY20 Requested Items and Estimated Cost

HUES	Bathroom Flooring	$ 5,000 (end of life)
	Water Heater Replacement	$ 6,000 (propane heater is not an option)
	Stair Treads-Phase 2	$ 8,000 (2nd of two phases – safety issues)
	Muenters Unit Roof	$ 35,021 (deferred for two years to accommodate HSTEP)
	Solar Panel Roofing	$ 9,142 (total cost was over $90k)
	HUES Sub-Total	**$ 63,163**
HPS	Fire Alarm Upgrades	$ 25,000 (upgrades needed to keep system current)
	Chair Replacements-Phase 1	$ 5,440 (chairs are falling apart)
	Classroom Cabinets-Phase 1	$ 5,060 (needed storage)
	Library Carpet	$ 9,858 (end of life)
	Flooring (Rm 117/Nurse)	$ 12,500 (end of life)
	Shades for New Windows	$ 5,200 (needed as a result HSTEP)
	Heating Control Unit	$ 21,999 (unexpected failure)
	HPS Sub-Total	**$ 85,057**
HPS/HUES FY20 Water Testing		$ 3,000 (required to test every year for 3 years)
	Total	**$151,220**

Hollis School Building Expendable Trust

Current Balance:	$ 119,509
To be added in FY20:	$ 120,000
FY20 Expenditures:	$ 151,220
Resulting Balance:	$ 88,289

SAU Building Expendable Trust

Background

The four most pressing needs for the SAU property are:

- Security upgrades
- Landscaping issues
- Interior painting
- Bathroom upgrades (on hold until SAU barn plans completed)

FY20 Requested Items/Estimated Cost - $20,000

1. **Security Upgrades: Estimated Cost: $12,000**
   - ✓ Install FOB system for building entry
   - ✓ Install three security cameras (2 outdoor/1 Indoor) and monitor

2. **Landscaping Issues: Estimated Cost: $5,000**
   - ✓ Remove dying tree at parking lot edge
   - ✓ Install weed fabric, shrubs and rocks to beds

3. **Interior Painting: Estimated Cost: $3,000**
   - ✓ Main entrance painting and three other rooms

SAU Building Expendable Trust

Current Balance:	$ 22,782
To be added in FY20:	$ 23,970
FY20 Expenditures:	$ 20,000
Resulting Balance:	$ 26,752

HSD Water System Expendable Trust

Emergency service and repairs to the water system at the Rocky Pond location in January and March 2019 **Total Cost: $5,051.34**

Current Balance:	$ 50,000
To be added in FY20:	$ 0
FY19 Expenditures:	$ 5,052
Resulting Balance:	$ 44,948

Charter
Hollis School District
Facilities Working Group

1. PURPOSE

As part of its on-going Capital Improvements planning, the **Hollis School District** is seeking improvements to its facilities at 4 Lund Lane, Hollis Primary School and Hollis Upper Elementary School.

The **Hollis School Board** recognizes that the 'farm house' at 4 Lund Lane, leased for SAU41 administration over many years, is minimally suitable for professional offices, while the attached 'barn' is unsuitable for any purpose. Preliminary studies indicate that a thoughtful renovation could result in a cost-effective transformation of these structures while retaining the historic rural character prioritized in the Town of Hollis Master Plan.

In parallel, the Board also recognizes that making further energy-efficiency enhancements at HPS and HUES, as identified during the HSTEP project, would confer valuable benefits for our schools: additional long-term energy savings, substantial improvements of the learning and working environment, and extension of life-span for both buildings.

The Board appoints the Facilities Working Group to undertake further study of these interests and to derive a capital improvement plan component for them.

FUNDING

The Board received a mandate to pursue these matters through Article 3 of the FY2020 Warrant, which passed by unanimous vote at the March 2019 Hollis School District Annual Meeting:

> *Article 3 (as amended): To see if the Hollis School District will vote to raise and appropriate the sum of $64,600 to create the design development of the proposed renovation primarily of the School Administrative Unit 41 barn and secondarily of the associated building at 4 Lund Lane and to provide estimated costs for additional energy saving projects in the school buildings. This is a special warrant article pursuant to RSA 32:3, VI (d)*.

2. CHARTER

The Board establishes the Facilities Working Group as an advisory committee to pursue the goals identified in Article 3, including the development of project plans and RFQs, and to deliver quote-based recommendations reflecting true project costs to the Board.

The Group is to include the following appointments:

Hollis School Board	Tammy Fareed	Rob Mann, Chair, Advisory
Hollis Energy Committee	Eric Ryherd	Paul Happy
Holli Budget Committee	Mike Leavitt	
SAU 41	Andy Corey Superintendent	Kelly Seeley B.A.
Hollis Schools	Ed Hinkley HUES facilities	Chuck Stohl HPS facilities
Lead Contractors	Dave Ely Architect	Dick Henry Energy Consultant

SCOPE

Facilities Working Group tasks will be carried out within the framework of the District's FY21 budget process, leading to finalized recommendations for the FY21 Warrant. Progress will be reported periodically in Board meetings, public forum(s), and public hearing(s).

A. Generally, the Facilities Working Group is expected to take into account

a) renovation(s) of the 'barn' versus demolition
b) renovation(s) of the 'farm house' as office space
c) disposition of the land at 4 Lund Lane
d) additional energy efficiency improvements at HPS and/or HUES
e) capital improvement items identified by the CIP, giving special consideration to budgeting and scheduling opportunities or concerns

B. Lifespan of Facilities Working Group

- Commence work June 2019
- Should the Board vote to take no action on the proposed project(s), the Group would disband by December 31, 2019
- Should the Board vote to pursue a significant project, the Group will continue to help develop the appropriate warrant article(s), then disband after the District Annual Meeting in March 2020.

Windy Hill Associates

David Ely, AIA ■ 243 Clark Hill Rd., New Boston, NH 03070 ■ 603-487-5252

Hollis School Board
Barn and Office Renovation Scope and HSTEP Completion

May 15, 2019

Scope included in Architect's proposal dated December 21, 2018, revised January 3, 2019.

- Barn Upgrade
  - Raise structure and shift slightly for access.
  - New Foundation.
  - New Basement for file storage.
  - Renovate main and upper floors for meeting and office spaces.
  - New siding, roofing, insulation, doors and windows.

- Existing Office Renovations
  - Minor non-structural work to shift offices and better flow.

Additional scope items discussed at March 27, 2019 meeting:

- Complete renovation to existing offices for like-new commercial feel to all spaces. Could include:
  - Major renovation to existing offices for better function and more even distribution of spatial allocations.
  - Upgraded HVAC system.
  - New insulation at existing offices.
    - Insulate from inside requires new drywall.
    - Insulate from outside requires new siding.
  - New windows at existing offices.
  - Tear-down one-story and re-build two story link between offices and barn (Ell, current stair and conference room). This adds 720 sq. ft. of second floor space and would be a good location for an elevator.
- Elevator required?
  - For barn renovations and basic renovations to office building the elevator may not be required. If renovations are more extensive it will be.
- Work could be phased.
  - Barn foundation concurrent with completing HSTEP renovations.
  - Or finish barn then renovate existing offices.
- Coordinate solar panels with Dick Henry and Eric Ryherd

- Need comparative analysis for complete renovation vs tear-down and re-build based on square foot estimates.

HSTEP items to complete:

- 13 classrooms with unit ventilators to be upgraded to ASHP heat and air.
- Complete room air balancing during summer.
- $5,000 in budget for consultants to complete HSTEP. For Dick, John and Dave.
- Have John Penney talk with Mitsubishi rep who says we might not need as many outdoor units to complete the project.
- Reconsider removing one boiler, keep both as back-up. Is it worth the expense to consolidate?
- Consider converting to propane to get rid of underground oil tanks.
- Consider adding heat/air to corridors.

Additional projects:

- Sprinkler system for HPS – could be lease to purchase.
- Complete door replacement project.
- HBMS expansion of Robotics shop and renovation of science and wood-shop classrooms.

Cost comparison to Upgrade SAU offices.

15-May-19

Office area	3,836 sq. ft.
Barn area	2,967 sq. ft.
Total area	6,803 sq. ft.

Minor renovations to offices	3,836 sq ft x $100/Sq. ft.	$383,600
Renovate Barn	Estimate	$700,000
Elevator	Estimate	$115,000
Total	Estimate	**$1,198,600**

Note: In this scenario the elevator may not be required.

Gut rehab existing offices	3,836 sq ft x $200/sq ft	$767,000
Renovate Barn	Estimate	$700,000
Elevator	Estimate	$115,000
Total	Estimate	**$1,582,000**

Note: the foundation of the Ell is suspect and may need to be replaced.

Gut rehab existing offices replace Ell	*	$1,070,000
Renovate Barn	Estimate	$700,000
Elevator	Estimate	$115,000
Total	Estimate	**$1,885,000**

* 3,115 sq ft renovations x $200	$623,000
* Demo Ell $15,000	$15,000
* New 2 story Ell 1,440 sq ft x $300	$432,000
	$1,070,000

This option adds 720 sq ft total 7,500 sq ft and gives a good place for the elevator.

Demo office only	Estimate	$30,000
Site work	Estimate	$75,000
New Office building	3,836 sq ft x $300 /sq ft	$1,150,000
Renovate Barn	Estimate	$700,000
Elevator	Estimate	$115,000
Total	Estimate	**$2,070,000**

Demo office and Barn	Estimate	$35,000
Site work	Estimate	$80,000
New Office Building	6,800 sq ft x $300 per sq ft	$2,040,000
Elevator	Estimate	$115,000
Total	Estimate	**$2,270,000**

Hollis School Board Policy Committee

To: Andy Corey
From: Hollis School Board Policy Committee
RE: Policy Recommendations
Date: May 20, 2019

The HSB Policy Committee makes the following recommendations for the June 5, 2019 School Board meeting:

Present for a ***Third Reading***:

1. AC: Non-Discrimination
2. GBA: Equal Opportunity Employment

Present for a ***Second Reading***:

1. JFAB: Admission of Tuition and Nonresident Students
2. ADB/GBEC: Drug Free Workplace
3. ADC/GBED: Tobacco Products Ban
4. KDCA: Information Distribution and Display (replace with current KHC)
5. GCPA: Reduction in Instructional Staff Work Force

Present for a ***First Reading***:

1. DJ: Purchasing
2. DJB: Purchasing Procedures
3. EHAB: Data Governance and Security
4. BEDG: Minutes
5. BEDH: Public Participation at Board Meetings

AC

Category R

NON-DISCRIMINATION

It is the policy of the Board that there will be no discrimination on the basis of age, gender, race, creed, color, religion, marital status, sexual orientation, gender identity, national or ethnic origin, economic status, or disability for employment in, participation in, admission/access to, or operation and administration of any educational program or activity in the School District.

The Superintendent or his/her designee will receive all inquiries, complaints, and other communications relative to this policy and the applicable laws and regulations concerned with non-discrimination.

This policy of non-discrimination is applicable to all persons employed or served by the District. Any complaints or alleged infractions of the policy, law or applicable regulations will be processed through the grievance procedure. This policy implements PL 94-142, Section 504 of The Rehabilitation Act of 1973, Title II of The American with Disabilities Act, Title VI or VII of The Civil Rights Act of 1964, Title IX of The Education Amendments of 1972, and the laws of New Hampshire pertaining to non-discrimination.

Legal References:

RSA 354-A:6, Opportunity for Employment without Discrimination a Civil Right

RSA 354-A:7, Unlawful Discriminatory Practices

The Age Discrimination in Employment Act of 1967

Title II of The Americans with Disabilities Act of 1990

Title VII of The Civil Rights Act of 1964 (15 or more employees)?

Appendix: AC-R

Revised: September 2008
Revised: July 1998, February 2004, February 2005
1st reading: August 8, 2012
2nd reading: September 12, 2012
3rd reading: Waived
Approved: September 12, 2012
1st Reading: April 3, 2019
2nd Reading: May 1, 2019
3rd Reading: June 5, 2019

GBA

Category R
See also AC

EQUAL OPPORTUNITY EMPLOYMENT

The Hollis School District will recruit and consider candidates without regard to gender, sexual orientation, gender identity, race, creed, color, religion, marital status, nationality, ethnic origin, economic status, age, or disability. When there are opportunities for promotions and qualifications are equal, consideration will be given first to employees.

The District will employ individuals who meet the physical and mental requirements, and who have the education, training, and experience established as necessary for the performance of the job without regard to gender, sexual orientation, gender identity, race, creed, color, religion, marital status, nationality, ethnic origin, economic status, age, or disability, except for reasons related to ability to perform the requirements of the job.

Inquiries, complaints, and other communications relative to this policy and to the applicable laws and regulations concerned with non-discrimination shall be received by the Superintendent or his/her designee.

This policy of non-discrimination is applicable to all persons employed or served by the district. Any complaints or alleged infractions of the policy, law or applicable regulations will be processed through the grievance procedure. This policy implements PL 94-142, Section 504 of the Rehabilitation Act of 1973, Title II of the American with Disabilities Act, Title VI or VII of the Civil Rights act of 1964, Title IX of the Education Amendments of 1972, and the laws of New Hampshire pertaining to non-discrimination.

Legal Reference:

RSA 354-A:7, Unlawful Discrimination Practices

Adoption: March 9, 2006

1st Reading: August 10, 2016

2nd Reading: September 7, 2016

3rd Reading: Waived

Adopted: September 7, 2016

1st Reading: April 3, 2019

2nd Reading: May 1, 2019

3rd Reading: June 5, 2019

JFAB

Category P

ADMISSION OF TUITION AND NONRESIDENT STUDENTS

I. Residency

Residency for the purpose of enrollment in our School District (hereafter referred to as the District) shall be defined by RSA 193:12. Any student who meets the RSA 193:12 definition of legal resident of this District is entitled to attend school in this District. A student who is not a legal resident of the District may attend school in the District only with the consent of the Superintendent. Disputes regarding residency shall be determined by the relevant laws in effect at the time.

II. Admission of Non-Resident Students

Individual non-resident students may be considered for admission to the District only under the following four stated conditions:

1. A resident student who moves from the District during the school year may continue as a non-resident student through the end of the school year. The District of Residence must agree to pay the tuition rate (as calculated in Section III), pro-rated, for the time that they are not legal residents of our District, plus agree to be responsible for special education costs. However, if the resident student moves from the District after March 31, the tuition and the need for an agreement with the District of Residence will be waived.

2. Non-resident students who are children of employees of the Hollis School District or the SAU 41 Office, may attend the District if space is available. These students are not exempt from the requirement to have an agreement with their District of Residence, regarding payment of special education costs, prior to admission. Employees should submit requests for admission of their non-resident student to the Building Principal no later than May 15th of the preceding school year and each school year thereafter. If there are more applicants than available spaces, students currently attending a particular school will have preference over a student who is not currently attending that particular school. Otherwise, the determination will be made by lottery. The Superintendent shall notify employees whether or not their child(ren) can be accommodated by July 15th. Successful applicants shall pay 25% of the tuition rate as calculated in Section III. Employees who leave employment within the SAU 41 office or the District must withdraw their child(ren) at the time of their departure unless the new district of residence agrees to pay the tuition rate as calculated in Section III, (pro-rated) and any special education costs for the remainder of the school year.

The availability of space in a particular program or class shall be determined by the Superintendent/designee and shall include consideration of the overall number of students in that program or class, any applicable state or local mandates for program or class size, the particular demands on teacher time presented by students currently scheduled for that program or class, a reasonable estimate of the number of new resident students who may join that program or class during the school year in question, and any other relevant criteria.

3. Students from other countries, who are the guests of District residents and participating in a federally recognized education exchange program, may be admitted if space is available.

Admitted students will not be charged tuition, but the District will not provide such students with special education, English as a Second Language, post secondary or other special programs.

4. Children of non-resident parents, who will be moving into the District during the school year, may be admitted prior to actual establishment of residency, provided a written request and verification of the anticipated date of residency are submitted to and approved by the Superintendent. There must also be a written agreement between the District and the student's school district of residence regarding payment of tuition (as calculated in Section III), pro-rated, and special education costs for the period of time that the student is not a resident of our District. Such request shall be supported by appropriate documentation such as a bona fide lease or a purchase and sale agreement, properly executed. Tuition charges will be waived at the sole discretion of the Hollis School Board if residence is established by October 1 of the same school year in which the child is enrolled.

In the above four circumstances, admission may be denied to any non-resident student who has been suspended or expelled, or involved in suspension or expulsion proceedings, in another District or whose behavior while a student in the District has had, in the sole judgment of the Superintendent, a negative impact on the resident students of the District. The decision to admit each non-resident student shall be made annually by the Superintendent and the decision of the Superintendent shall be final.

III. Tuition for Non-Resident Students

For the purpose of determining the tuition rate, the cost per pupil as reported on the MS 25/DOE 25 will be used. A signed tuition agreement, approved by the Superintendent, shall be on file in the SAU #41 office prior to attendance. Tuition, where applicable, shall be pre-paid in quarterly installments. Tuition shall not be reimbursed if the student leaves the District, voluntarily or involuntarily, during the period for which payment has already been made. Failure to pay tuition as due shall be grounds for revoking the admission of non-resident tuition students. Section IV below outlines limited special circumstances under which tuition may be waived.

IV. Responsibility for Services not Included in the Calculation of the Tuition Rate

The District will not provide transportation to any non-resident students. NH State Law guides the District's view of the responsibility for the provision of Special Education Services. Section 186-C: 13 states that "All expenses incurred by a school district in administering the law in relation to education for educationally disabled children shall be paid by the school district where the child resides".

V. Tuition Agreements with other School Districts

The District may enter into one or more agreements with other school districts or agencies for the admission of non-resident students with payment of tuition by the sending district or agency. The admission of such students under these circumstances shall be governed by the terms of said agreements.

VI. Other Situations

It is not possible to anticipate all situations that may arise. Notwithstanding any provision of this policy, the District reserves the right to charge tuition or to deny admission to any non-resident student. The District also reserves the right to admit non-resident students and waive tuition in situations not discussed in this policy.

Legal References:

RSA 186-C: 13, Special Education; Liability for Expenses

RSA 193:3, Change of School or Assignment

RSA 193:12, Legal Residence Required

1st Reading: September 12, 2012

2nd Reading: May 13, 2013

3rd Reading: July 11, 2013

Adopted: July 11, 2013

1st Reading: May 1, 2019

2nd Reading: June 5, 2019

Category R

DRUG-FREE WORKPLACE & DRUG-FREE SCHOOLS

A. Drug-Free Workplace

1. All District workplaces are drug- and alcohol-free. All employees and contracted personnel are prohibited from:

   a. Unlawfully manufacturing, dispensing, distributing, possessing, using, or being under the influence of any controlled substance or drug while on or in the workplace, including employees possessing a "medical marijuana" card.

   b. Distributing, consuming, using, possessing, or being under the influence of alcohol while on or in the workplace.

2. For purposes of this policy, a "controlled substance or drug" means and includes any controlled substance or drug defined in the Controlled Substances Act, 21 U.S.C. § 812(c), or New Hampshire Controlled Drug Act RSA 318-B.

3. For purposes of this policy, "workplace" shall mean the site for the performance of work, and will include at a minimum any District building or grounds owned or operated by the District, any school-owned vehicle, and any other school-approved vehicle used to transport students to and from school or school activities. It shall also include off-school property during any school-sponsored or school-approved activity, event or function such as a field trip or athletic event where students are under the jurisdiction, care or control of the District.

4. As a condition of employment, each employee and all contracted personnel will:

   a. Abide by the terms of this policy respecting a drug- and alcohol-free workplace, including any administrative rules, regulations or procedures implementing this policy; and

   b. Notify his or her supervisor of his or her conviction under any criminal drug statute, for a violation occurring on District premises or while performing work for the District, no later than five (5) days after such conviction.

5. In order to make employees aware of dangers of drug and alcohol abuse, the District will endeavor to:

   a. Provide each employee with a copy of the District drug- and alcohol-free workplace policy;

   b. Post notice of the District drug- and alcohol-free workplace policy in a place where other information for employees is posted;

   c. Establish a drug-free awareness program to educate employees about the dangers of drug abuse and drug use in the work place, the specifics of this policy, including, the consequences for violating the policy, and any information about available drug and alcohol counseling, rehabilitation, reentry, or other employee-assistance programs.

B. District Action Upon Violation of Policy

An employee who violates this policy may be subject to disciplinary action; up to and including termination of employment. Alternatively, the Board may require an employee to successfully complete an appropriate drug- or alcohol-abuse, employee-assistance rehabilitation program.

The Board will take disciplinary action with respect to an employee convicted of a drug offense in the workplace, within thirty (30) days of receiving notice of a conviction. Should District employees or contracted personnel be engaged in the performance of work under a federal contract or grant, or under a state contract or grant, the Superintendent will notify the appropriate state or federal agency from which the District receives contract or grant moneys of an employee/contracted personnel's conviction, within ten (10) days after receiving notice of the conviction.

The processes for disciplinary action shall be those provided generally to other misconduct for the employee/contractor personnel as may be found in applicable collective bargaining agreements, individual contracts, School Board policies, contractor agreements, and or governing law. Disciplinary action should be applied consistently and fairly with respect to employees of the District and/or contractor personnel as the case may be.

C. Drug-Free School Zone

Pursuant to New Hampshire's "Drug-Free School Zone" law (RSA Chapter 193-B), it is unlawful for any person to manufacture, sell prescribe administer, dispense, or possess with intent to sell, dispense or compound any controlled drug or its analog, within a "drug-free school zone". The Superintendent is directed to assure that the District is and remains in compliance with the requirements of RSA 193-B, I, and N.H. Ed. Part 316 with respect to establishment, mapping and signage of the drug-free zone around each school of the District.

D. <u>Implementation and Review</u>

a. The Superintendent is directed to promulgate administrative procedures and rules necessary and appropriate to implement the provisions of this policy.

b. In order to maintain a drug-free workplace, the Superintendent will perform a biennial review of the implementation of this policy. The review shall be designed to (i) determine and assure compliance with the notification requirements of section A.5.a, b and d; (ii) determine the effectiveness of programs established under paragraph A.5.c above; (iii) ensure that disciplinary sanctions are consistently and fairly enforced; and (iv) and identify any changes required, if any.

<u>Legal References:</u>

- *RSA Chapter 193-B Drug Free School Zones*
- *41 U.S.C. §101, et. Seq. - Drug-free workplace requirements for Federal contractors, and Federal grant recipients*
- *N.H. Admin. Code, Ed. Part 316*

Adopted: May 13, 2004
Reviewed:
1st Reading: June 1, 2016
2nd Reading: July 18, 2016
3rd Reading: July 18, 2016 (Waived)
Adopted: July 18, 2016

1st Reading: May 1, 2019
2nd Reading: June 5, 2019

Category R

TOBACCO PRODUCTS BAN USE AND POSSESSION IN AND ON SCHOOL FACILITIES AND GROUNDS

State law prohibits the use of any tobacco product, E-cigarette, or liquid nicotine in any facility or upon any grounds maintained by the District.

A. Definitions

"Tobacco product(s)" means any product containing tobacco including, but not limited to, cigarettes, smoking tobacco, cigars, chewing tobacco, snuff, pipe tobacco, smokeless tobacco, and smokeless cigarettes as well as any other product or item included in RSA 126-K:2, XI as the same may be amended or replaced from time to time.

"E-cigarette" means any electronic smoking device composed of a mouthpiece, a heating element, a battery, and electronic circuits that provides a vapor of pure nicotine mixed with propylene glycol to the user as the user simulates smoking. This term shall include such devices whether they are manufactured as e-cigarettes, e-cigars, or e-pipes, or under any other product name as well as any other product or item included in RSA 126-K:2, II-a as the same may be amended or replaced from time-to-time.

"Liquid nicotine" means any liquid product composed either in whole or in part of pure nicotine and propylene glycol and manufactured for use with e-cigarettes, as well as any other product or item included in RSA 126-K:2, III-a as the same may be amended or replaced from time-to-time.

"Facility" is any place which is supported by public funds and which is used for the instruction of students enrolled in preschool programs and in all grades maintained by the District. This definition shall include all administrative buildings and offices and areas within facilities supportive of instruction and subject to educational administration, including, but not limited to, lounge areas, passageways, rest rooms, laboratories, classrooms, study areas, cafeterias, gymnasiums, maintenance rooms, and storage areas.

B. Students

No student shall purchase, attempt to purchase, possess or use any tobacco product, E-cigarette, or liquid nicotine in any facility, in any school vehicle or anywhere on school grounds maintained by the District.

Enforcement of the prohibition against students shall initially rest with building principals, or their designees, who may report any violation to law enforcement, for possible juvenile, criminal or other proceedings as provided under state law. Additional consequences may be administered pursuant to printed student conduct rules.

C. Employees

No employee shall use any tobacco product, E-cigarette, or liquid nicotine in any facility, in any school vehicle or anywhere on school grounds maintained by the District.

Initial responsibility for enforcement of this prohibition shall rest with building principals, or their designees. Any employee(s) who violate(s) this policy is subject to disciplinary action which may include warning, suspension or dismissal. Violations may also be referred to appropriate law enforcement and/or other appropriate agencies for criminal or other proceedings as provided under state law

D. All other persons

No visitor, contractor, vendor or other member of the public shall use any tobacco products, E-cigarette, or liquid nicotine in any facility, in any school vehicle, or anywhere on school grounds maintained by the District.

Building administration, and where appropriate, other site supervisor or their designee(s), shall have the initial responsibility to enforce this section, by requesting that any person who is violating this policy to immediately cease the use of tobacco products, E-cigarette or liquid nicotine. After this request is made, if any person refuses to refrain from using such products in violation of this policy, the principal, site supervisor, or designee may call contact the appropriate law enforcement agency(ies) for possible criminal or other proceedings as provided under state law.

E. Implementation and Notice - Administrative Rules and Procedures.

The Superintendent shall establish administrative rules and procedures to implement this policy, which rules and procedures may be building level and/or district-wide. Rules and procedures relating to student violations and resulting disciplinary consequences should be developed in consultation with building principal(s).

The Superintendent, working with the building principal(s), shall provide annual notice to employees, students and parents of the pertinent provisions of this policy (e.g., student or staff handbook) along with applicable administrative regulations and procedures, which may include prescribed consequences for violations of this policy. Such notice should include information that violation of this Policy could lead to criminal or other such proceedings.

Signs shall be placed by the District in all buildings, facilities and school vehicles stating that the use of tobacco products is prohibited.

Legal References

RSA 155:64 - 77(Indoor Smoking Act)

RSA 126-K:2, Definitions

RSA 126 - K:6 (Possession and Use of Tobacco Products by Minors)

RSA 126 K:7 (Use of Tobacco Products on Public Educational Grounds Prohibited)

1st Reading: June 1, 2016 (amended)
2nd Reading: July 18, 2016
3rd Reading: July 18, 2016 (Waived)
Adopted: July 18, 2016
1st Reading: May 1, 2019
2nd Reading: June 5, 2019

KDCA

Category R

INFORMATION DISTRIBUTION AND DISPLAY

This policy governs what types of information may be allowed to be distributed via students, posted on bulletin boards, displayed in the school, or distributed in other ways to students and to their families through the school district.

Non-Discrimination;

All organizations wishing to distribute or display information must practice a policy of non-discrimination for participation that is comparable to the high standards in place for the Hollis School District.

Information distributed via students;

All information distributed via students must be from a non-profit organization that is affiliated with the Town of Hollis, the Hollis School District or another district within SAU 41 and must be pre-approved by the Superintendent.

Information Distributed or Displayed in Other Manners:

All organizations that wish to distribute or display information in other manners approved by the Superintendent or School Board must be non-profit and the activity must be student-related.

Votes:

All information distributed or displayed concerning district or town votes or meetings at which there is to be voting, or information concerning voting, must be neutral and factual.

Information that is not School Sponsored:

All information distributed or displayed that is not school sponsored must clearly state that it is not school sponsored.

Approval Process:

All information for distribution or display by any organization must be submitted to the superintendent's office for prior approval accompanied by the Approval for Information Distribution or Display form. This form is available via the SAU website and the school offices. The Superintendent and the School Board reserve the right to refuse requests for the distribution or display of such information, on a case-by-case basis.

Adoption: December 9, 2004

1st Reading: February 9, 2006

2nd Reading: February 14, 2006

Re-adoption: March 9, 2006

1st Reading: May 1, 2019

2nd Reading: June 5, 2019

GCPA

Category O

REDUCTION IN INSTRUCTIONAL STAFF WORK FORCE

A. When it is determined to reduce the number of professional teaching staff, the following procedure will be utilized:
   1. As soon as a reduction-in-force becomes necessary the President of the Association shall be notified in writing, specifying the nature of the proposed reduction.
   2. Reductions will first be accomplished by attrition (resignations, retirements, refusal to contract).
   3. If more reductions-in-force are necessary, then part time Staff shall be laid off.
   4. For purposes of this policy, classifications will be defined as follows:
      a. Regular education pre-school through 6^{th} grade.
      b. Specialized teaching areas including, but not limited to, Special Education, Art, Computer, Guidance, Nurses, Library, Music (General, Choral, or Instrumental), Physical Education, Reading and Math Specialists, Spanish, Environmental Science and School Psychologist.
   5. Within these classifications, probationary teachers shall be laid off first. If further reductions are necessary, then teachers on continuing contract will be laid off. A continuing contract teacher is one who qualifies for notice, reasons, and a School Board hearing under the provisions of RSA 189:14-a. Among continuing contract teachers, the following criteria will be utilized:
      a. New Hampshire Certification.
      b. Academic and professional preparation beyond minimum requirements.
      c. Teaching performance as determined by previous evaluations.
   6. If the factors set forth in paragraph A.5 are substantially equal, then seniority shall determine the order of layoff, with the least senior teacher being laid off first. Seniority is defined as the total years of uninterrupted service to the Hollis School District within a bargaining unit position. Approved leaves or transfers to a non-bargaining unit position shall not result in loss of previously accrued seniority. However, resignation shall terminate all previously accrued seniority.

B. Teachers shall be recalled in reverse order of layoff for any open position within the classification in which the layoff occurred. Only continuing contract teachers shall be eligible for recall rights. The same conditions as A.4 shall apply to the recall.
   1. Laid off teachers shall be eligible for recall for a two (2) year period following their final date of employment.
   2. Teachers shall be responsible for notifying the Superintendent in writing of their current address. Recall notices shall be mailed certified, return receipt requested.

3. Teachers shall have twenty (20) business days to respond to any recall notice. Failure to accept recall to a permanent full-time position shall terminate the teacher's rights under this Article.
4. No new employees shall be hired for any vacancy within a classification while there are laid off personnel from those classifications available to fill those positions.
5. Teachers recalled shall retain previous seniority and other accrued contract benefits, such as accumulated sick leave.
6. Should a vacancy occur within a classification and there are no teachers on the recall list for that classification, then that vacancy shall be offered to the most senior teacher laid off from another classification who is certified and substantially qualified to teach that position. If the laid off teacher refuses the vacant position, his/her recall rights shall be retained.

This policy is referenced in the Collective Bargaining Agreement in Article X, Working Conditions (10.8) and Appendix C.

1st Reading: July 12, 2005

2nd Reading: October 20, 2005

Adoption: March 9, 2006

1st Reading: May 1, 2019

2nd Reading: June 5, 2019

DJ

Category R

PURCHASING

The acquisition of supplies, equipment, and services will be centralized in the business office, which functions under the supervision of the Superintendent or his/her designee, and through whose office all purchasing transactions are conducted.

The Hollis School Board assigns the Superintendent the responsibility for the quality and quantity of purchases made. The prime guidelines governing this responsibility are that all purchases fall within the framework of budgetary limitations and that they be consistent with the approved educational goals and programs of the Hollis School District.

The Business Administrator shall be responsible for all phases of purchasing in accordance with Board policy; for requisitions, current order purchasing, writing of specifications for bids, deliveries, storage, and other tasks related to the purchases, acceptance and distribution of supplies.

No contract or purchase order is valid without the approval of the Business Administrator.

Legal Reference:

RSA 194-C:4 II (a), Superintendent Services

NH Code of Administrative Rules, Section 303.01 (b), Substantive Duties of School Boards

1st Reading: May 12, 2005

2nd Reading: August 4, 2005

Adoption: March 9, 2006

1st Reading: June 5, 2019

DJB

Category O

PURCHASING PROCEDURES

Procedures for purchasing will be developed by the Superintendent or his/her designee.

Purchasing procedures will be designed to avoid assumption of risk and to ensure the best possible price for the desired products and services**.**

These procedures will require that all purchases are made on properly approved purchase orders and that for items not put to bid, price quotations will be solicited.

Special arrangements may be made for ordering perishable and emergency supplies.

Legal References:

RSA 194-C:4 II (a), Superintendent Services

NH Code of Administrative Rules Section 303.01 (b), Substantive Duties of School Boards

1st Reading: June 5, 2019

EHAB

Category: Priority/Required by Law
Related Policies EHAA, EHB, GBEBD, GBEF, IHBH, JICJ, JICL, JICM, KD, & KDC

DATA GOVERNANCE AND SECURITY

To accomplish the District's mission and comply with the law, the District must collect, create and store information. Accurately maintaining and protecting this data is important for efficient District operations, compliance with laws mandating confidentiality, and maintaining the trust of the District's stakeholders. All persons who have access to District data are required to follow state and federal law, District policies and procedures, and other rules created to protect the information.

The provisions of this policy shall supersede and take precedence over any contrary provisions of any other policy adopted prior to the date of this policy.

A. Definitions

Confidential Data/Information - Information that the District is prohibited by law, policy or contract from disclosing or that the District may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information regarding students and employees.

Critical Data/Information - Information that is determined to be essential to District operations and that must be accurately and securely maintained to avoid disruption to District operations. Critical data is not necessarily confidential.

B. Data and Privacy Governance Plan - Administrative Procedures.

1. Data Governance Plan. The Superintendent, in consultation with the District Information Security Officer ("ISO") (see paragraph C, below) shall create a Data and Privacy Governance Plan ("Data Governance Plan"), to be presented to the Board no later than June 30, 2019. Thereafter, the Superintendent, in consultation with the ISO, shall update the Data Governance Plan for presentation to the Board no later than June 30 each year.

The Data Governance Plan shall include:

(a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use;

(b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed minimum standards set by the New Hampshire Department of Education;

(c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools, and extensions used on District hardware, server(s) or through the District network(s);

(d) A response plan for any breach of information; and

(e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

2. Policies and Administrative Procedures. The Superintendent, in consultation with the ISO, is directed to review, modify and recommend (policies) create (administrative procedures), where necessary, relative to collecting, securing, and correctly disposing of District data (including, but not limited to Confidential and Critical Data/Information, and as otherwise necessary to implement this policy and the Data Governance Plan. Such policies and/or procedures will may or may not be included in the annual Data Governance Plan.

C. Information Security Officer.

The Network Administrator and the Database Manager are hereby designated as the District's Information Security Officer (ISOs) and report directly to the Superintendent or designee. The ISOs are responsible for implementing and enforcing the District's security policies and administrative procedures applicable to digital and other electronic data, and suggesting changes to these policies, the Data Governance Plan, and procedures to better protect the confidentiality and security of District data. The ISOs will work with the both District and building level administrators and Data managers (paragraph E, below) to advocate for resources, including training, to best secure the District's data.

Any member of the full technology team (the ISOs, the Assistant Superintendent, and the Business Administrator) are the District's alternate ISO and will assume the responsibilities of the ISO when the ISOs are not available.

D. Responsibility and Data Stewardship.

All District employees, volunteers and agents are responsible for accurately collecting, maintaining and securing District data including, but not limited to, Confidential and/or Critical Data/Information.

E. Data Managers.

All District administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the District's data inventory. Data managers will monitor employee access to the information to ensure that confidential information is accessed only by employees who need the information to provide services to the District and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISOs in enforcing District policies and procedures regarding data management.

F. Confidential and Critical Information.

The District will collect, create or store confidential information only when the Superintendent or designee determines it is necessary, and in accordance with applicable law. The District will provide access to confidential information to appropriately trained District employees and volunteers only when the District determines that such access is necessary for the performance of their duties. The District will disclose confidential information only to authorized District contractors or agents who need access to the information to provide services to the District and who agree not to disclose the information to any other party except as allowed by law and authorized by the District.

District employees, contractors and agents will notify the ISOs or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise. The ISOs or designee will investigate immediately and take any action necessary to secure the information, issue all required legal notices and prevent future incidents. When necessary, the Superintendent, ISOs, or designee are authorized to secure resources to assist the District in promptly and appropriately addressing a security breach as stipulated in the Data Governance Plan

Likewise, the District will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure.

All District staff, volunteers, contractors and agents who are granted access to critical or confidential information/data are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of such confidential or critical data/information. All individuals using confidential and critical data/information will strictly observe all administrative procedures, policies and other protections put into place by the District including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information no longer needed in a confidential and secure manner.

G. Using Online Services and Applications.

District staff members are encouraged to research and utilize online services or applications to engage students and further the District's education mission. District employees, however, are prohibited from installing or using applications, programs or other software, or online system/website until the DGT (Data Governance Team) approves the vendor and the software or service used. Before approving the use or purchase of any such software or online service, the ISOs or designee shall verify that it meets the requirements of the law, Board policy, and the Data Governance Plan, and that it appropriately protects confidential and critical data/information. This prior approval is also required whether or not the software or online service is obtained or used without charge.

H. Training.

The ISOs will provide appropriate training to employees who have access to confidential or critical information to prevent unauthorized disclosures or breaches in security. All school employees will receive annual training in the confidentiality of student records, and the requirements of this policy and related procedures and rules.

I. Data Retention and Deletion.

The ISOs or designee shall establish a retention schedule for the regular archiving and deletion of data stored on District technology resources. The retention schedule should comply with, and be incorporated into the data/record retention schedule established under Policy EHB and administrative procedure EHB-R, including but not limited to, provisions relating to Litigation and Right to Know holds as described in Policy EHB.

J. Consequences

Employees who fail to follow the law or District policies or procedures regarding data governance and security (including failing to report) may be disciplined, up to and including termination. Volunteers may be excluded from providing services to the District. The District will end business relationships with any contractor who fails to follow the law, District policies or procedures, or the confidentiality provisions of any contract. In addition, the District reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

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

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

Legal References:

*15 U.S.C. §§ 6501-6506 * Children's Online Privacy Protection Act (COPPA)*
*20 U.S.C. § 1232g * Family Educational Rights and Privacy Act (FERPA)*
*20 U.S.C. § 1232h * Protection of Pupil Rights Amendment (PPRA)*
*20 U.S.C. § 1400-1417 * Individuals with Disabilities Education Act (IDEA)*
*20 U.S.C. § 7926 * Elementary and Secondary Education Act (ESSA)*
*RSA 189:65 * Definitions*
*RSA 186:66 * Student Information Protection and Privacy*
*RSA 189:67 * Limits on Disclosure of Information*
*RSA 189:68 * Student Privacy*
*RSA 189:68-a * Student Online Personal Information*
*RSA 359-C:19-21 * Right to Privacy/Notice of Security Breach*

District Policy History:

First reading: June 5, 2019

BEDG

Category R

MINUTES

The Secretary shall keep a record of the actions of Board meetings. The Board may provide a paid transcribing secretary to record minutes of meetings. The minutes of the Board shall be maintained, filed securely, and posted online available to the public. The minutes shall include all motions ad resolutions including the identification of each member who made a first and second of any motion. ~~kept in an official minute book and shall include resolutions and motions~~. Papers not a part of a formal motion may be omitted if they are referred to and identified by some method.

Copies of the draft minutes of a meeting shall be sent to the members of the Board before the meeting at which they are to be approved. Corrections to the minutes may be made at the meeting at which they are to be approved. Corrections shall appear in the official minutes and in the minutes of the meeting in which changes were made.

All minutes shall be kept in accordance with RSA 91-A:2 and 3 III and will be in the custody of the Superintendent, who will make them available no later than 144 hours after the meeting to interested citizens on request. (72 hours for minutes of non-public sessions)

Legal References:

RSA 91-A:3 III, Public Records and Meetings: Non-Public Sessions

RSA 91-A:4 I, Public Records and Meetings: Minutes and Records available for Public Inspection

RSA 91-A:2 II, Public Records and Meetings: Meetings Open to Public

Adoption: December 15, 2004

1st Reading; June 5, 2019

BEDH

Category R See Also KE, KEB

PUBLIC PARTICIPATION AT BOARD MEETINGS

The primary purpose of School Board meetings is to conduct the business of the Board as it relates to school policies, programs and operations. The Board encourages residents to attend Board meetings so that they may become acquainted with the operation and programs of the schools. All official meetings of the Board shall be open to the press and public. However, the Board reserves the right to meet and to adjourn or recess a meeting at any time. The Board also reserves the right to enter non-public session at any time, in accordance with the provisions RSA 91-A:3.

In order to assure that persons who wish to appear before the Board may be heard and, at the same time, it may conduct its meetings properly and efficiently, the Board adopts as policy the following procedures and rules pertaining to public participation at Board meetings:

Rules of Order

1. ~~There will be at least one public comment session of up to 15 minutes set aside for citizens to address the Board.~~ *The Board will provide a maximum of fifteen minutes to hear public comments at the the beginning of each regular Board meeting.* This period may be ~~abbreviated or~~ extended by a majority vote of the Board. *Additionally, the Board may include additional public comment period for specific agenda items with a time limit for public comment specified on the pertinent agenda.* ~~Members of the public may offer comments during the time allotted on the agenda.~~
2. *Individual* speakers will be allotted three minutes per person. *Speakers may not relinquish allotted time to another speaker. For specific meetings and/or specific agenda items, The Board may at the outset of the public comment period increase the individual time limit for all speakers.*
3. *The Chair will recognize speakers on a first come basis.*
4. *In order to comply with the minute requirements of RSA 91-A:2, II, speakers shall identify themselves clearly for the record.*
5. *Except as otherwise provided in this policy, members of the public may offer comments on agenda items or upon any other matter of public concern directly relating to the District's school policies, programs and operations. In the interest of preserving individual privacy and due process rights, the Board requests that comments (including complaints) regarding individual employees (other than the Superintendent) or individual students be directed to the Superintendent in accord with the complaint/grievance resolution processes set forth in School Board Policies KE and/or KEB. Complaints regarding the Superintendent, may be made either during public comment, or directed to the School Board Chair as described in Board Policy KEB.*
6. *Any comments which do not adhere to the above, or which disrupt the official business of the Board may be ruled out of order by the Chair. Repeated disruption may result in the individual being asked to leave the meeting. Obscene speech, comments threatening bodily harm, or other unprotected speech will not be tolerated.*
7. *The Board Chair may terminate the speaker's privilege of address if the speaker does not follow the above rules of order. Repeated violations or disruptions may result in the intervention of law enforcement, with the potential for criminal charges.*

~~Consistent with RSA 91-A:3, Policy BEDB, and the laws pertaining to student and family privacy rights, the Board will not place any matter on the public agenda that is to be properly discussed in a non-public session. Complaints regarding individual employees, personnel or students will be directed to the Superintendent in accord with Policies KE and KEB.~~

~~4. All speakers are to conduct themselves in a civil manner. Obscene, libelous, defamatory or violent statements will be considered out of order and will not be tolerated. The Board Chair may terminate the speaker's privilege of address if the speaker does not follow this rule of order.~~

~~Members of the public~~ *Persons appearing before the Board* are reminded that members of the Board are without authority to act independently as individuals in official matters~~. per Policy BBAA~~. Thus, questions may be directed to individual Board members, but answers must be deferred pending consideration by the full Board.

With the aim of maintaining focus on the issues in discussion, it is desired that all speakers strive to adhere to ordinary norms of decorum and civility.

Legal References:

RSA 91-A:2, Meetings Open to Public

RSA 91-A:3, Non-Public Sessions

U.S. Constitution, 1st Amendment

Revised: May 2007

Revised: July 1998, November 1999, February 2004

First Reading: October 10, 2012

Second Reading: December 12, 2012

Third Reading: April 10, 2013

Approved: April 10, 2013

1st Reading: June 5, 2019