

Brookline School Board
Wednesday, April 17, 2019
Captain Samuel Douglass Academy
6:00 PM

All Times are estimates and subject to change without notice

- 6:00 Call to Order
- 6:05 Agenda adjustments
Correspondence/Resignations/Nominations
- 6:10 Public Input
- 6:15 Public Hearing – Special Education Trust Fund**
- 6:30 Non-public under RSA 91-A: 3II (a) Compensation and/or (c) reputation —Administrative nominations, out of district tuition request
- 6:50 Principal Report
 - NWEA data presentation
- 7:10 Discussion
 - HB 1612 Governance Policy
 - Revenue and Expense Update
 - Board goals for 2019-2020
 - Kindergarten
 - Negotiations team
- 7:30 **Deliberations**
 - To see what action the Board will take regarding policy JH – Attendance, Absenteeism and Truancy – Second Reading
 - To see what action the Board will take regarding the administrations recommendation regarding the usage of special education trust fund
 - To see what action the Board will take regarding the Superintendent’s administrative nominations
 - To see what action the Board will take regarding the Administration’s recommendation for an out of district tuition
 - To see what action the Board will take regarding the Administration’s recommendation to accept the donation of a shed by the PTO/CSDA theater club for storage of materials
- 7:50 Approval of Minutes – March, 2019
- 8:00 Motion to adjourn

Public Hearing

on

Use of Special Education Trust Funds

Current Balance: \$125,000

FY20 Addition: \$50,000

7/1/19 Balance: \$175,000

Reason for Request

The District will incur an estimated \$82,464 in unexpected, unbudgeted special ed costs. At this point in the year, the District can cover all but \$11,369. It is possible we can cover it all but the administration would like to get the Board's direction if we can't cover it.

Estimated Year End Balance (as of 4/9/19)

Unreserved Fund Balance	\$113,631 Conservative estimate
Less Special Education Fund (FY20)	\$50,000
Less Facilities Maintenance Fund (FY20)	\$50,000
Less Contingency Fund (FY20)	\$25,000
Sub-Total	-\$11,369 *

* This amount could be less or even a positive number depending on how encumbrances play out in May and June

Possible Scenarios

During Budget Season, we told voters our estimated amount to return to taxpayers was \$35,000

Scenario #1

Use Special Ed Trust	\$10,000 Up to
Fund Balance to Reduce Taxes	-\$1,369 Assumes we'll have a higher EOY balance than at this time

Scenario #2

Use Special Ed Trust	\$20,000 Up to
Fund Balance to Reduce Taxes	\$8,631

Scenario #3

Use Special Ed Trust	\$30,000 Up to
Fund Balance to Reduce Taxes	\$18,631

Scenario #4

Use Special Ed Trust	\$40,000 Up to
Fund Balance to Reduce Taxes	\$28,631

Scenario #5

Use Special Ed Trust	\$50,000 Up to
Fund Balance to Reduce Taxes	\$38,631

Board Direction

- 1 Motion should include an "up to" number
- 2 Motion should include direction if EOY number can cover the entire special ed overage

Brookline Administrator's Report

April 17, 2019

Calendar, Events, Programs

April 2nd	PTO Meeting @ RMMS	May 14th	HB District Band Concert
April 4th	HBMS Incoming Grade 7 Parent Night	May 16th	Kaleidoscope Featuring
April 10th	Kindergarten Information Night		3rd Grade @ 6 p.m., HBHS
April 12th & 13th	CSDA Theater Club Production	May 18th	Brookline Bolt
April 17 th	Grade 1 Capital Center for the Arts @	Friday, May 17 th	Grade K - Davis Farmland
April 22nd - 26th	Spring Vacation	May 24th	Memorial Day Program
May 2nd	CSDA Spring Showcase	May 27th	School Closed - Memorial Day
May 3 rd	Progress Reports	May 29th	Chorus & Orchestra Concert
May 7 - 23	NH SAS Testing	May 30th	Spring Band Concert
May 9th	PTO Ice Cream Social at RMMS	May 30-31	Grade 2 - Discovery Museum

BSD:

Letters About Literature

NWEA Winter Results Recap

School-wide STEM Project

Theater Club Shed Donation

Policy Review

● JH - Attendance, Absenteeism and Truancy

BSD Enrollment Summary

Pre - 3	Pre-4	K	1	2	3	4	5	6
18	24	66 40 full 26 half [Full- Day classes 13, 13, 14, 2 half - day 13,13	76 16, 15, 15, 15, 15	77 18,19, 20, 20	71 23, 24, 24	85 21, 21, 21, 22	80 19, 20, 20, 21	77 19, 19, 19, 20

RMMS: 332

CSDA: 242

Brookline NWEA Cohort Study, 2015-2019

NWEA % At or Above Norm Grade Level Mean RIT > Reading

Year/ Grade	Spring 2015	Spring 2016	Spring 2017	Fall 2017	Winter 2018	Fall 2018	Winter 2019	Fall - Winter Cohort +/-	Winter- Winter Cohort +/-	Overall Cohort +/-
Two	N/A	N/A	N/A	N/A	83	N/A	80	N/A	N/A	N/A
Three	N/A	78.9	92.1	N/A	76.3	N/A	83	N/A	+0	N/A
Four	80.2	76.6	79.2	89.7	93.6	80.0	88.0	+8.0	+11.7	+11.7
Five	74.5	84.7	74.6	81.9	87.5	89.9	90.8	+0.9	-2.8	-1.3
Six	80.2	75.0	81.0	76.5	72.7	84.6	88.3	+3.7	+8	+9.4
Average	78.3	78.8	81.7	82.7	82.5	84.8	88.7	+3.9	+3.2	+6.6

NWEA % At or Above Norm Grade Level Mean RIT > Mathematics

Year/ Grade	Spring 2015	Spring 2016	Spring 2017	Fall 2017	Winter 2018	Fall 2018	Winter 2019	Fall - Winter Cohort +/-	Winter- Winter Cohort +/-	Overall Cohort +/-
Two	N/A	N/A	N/A	N/A	78.4	N/A	75	N/A	N/A	N/A
Three	N/A	80.3	86.8	N/A	76.3	N/A	79	N/A	0.6	N/A
Four	71.4	67.7	78.2	96.2	92.3	80.0	84.5	+4.5	+8.2	+8.2
Five	74.5	71.4	63.2	77.8	80.6	89.9	89.5	-0.4	-2.8	+2.7
Six	68.3	71.3	78.0	73.1	81.8	75.6	79.2	+3.6	-1.4	-1.1
Average	71.4	72.7	76.6	82.4	84.9	81.8	84.4	+2.6	+1.3	+3.3

Student Growth Summary Report

Aggregate by School

Term: Winter 2018-2019
District: SAU #41 (Hollis-Brookline SAU Office)

Norms Reference Data: 2015 Norms
Growth Comparison Period: Winter 2018 - Winter 2019
Weeks of Instruction: Start - 19 (Winter 2018)
 End - 16 (Winter 2019)

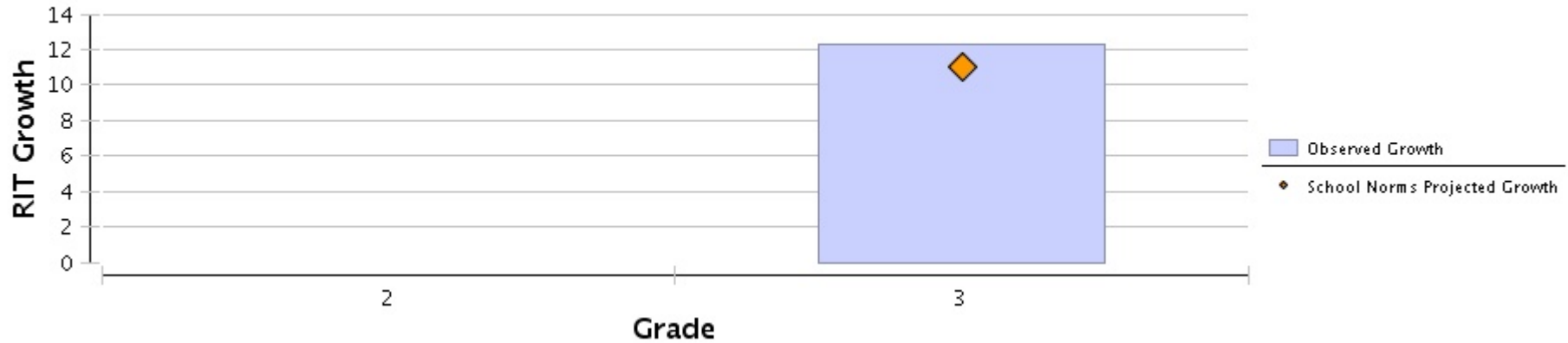
Grouping: None
Small Group Display: No

Richard Maghakian Memorial School

Mathematics

		Comparison Periods							Growth Evaluated Against							
		Winter 2018			Winter 2019			Growth		School Norms			Student Norms			
Grade (Winter 2019)	Growth Count‡	Mean RIT	SD	Percentile	Mean RIT	SD	Percentile	Observed Growth	Observed Growth SE	Projected Growth	School Conditional Growth Index	School Conditional Growth Percentile	Count with Projection	Count Met Projection	Percent Met Projection	Student Median Conditional Growth Percentile
2	0	**			**			**					**			
3	63	194.2	11.6	92	206.5	11.3	95	12.3	0.9	11.0	0.67	75	63	40	63	63

Mathematics



Explanatory Notes

** Calculations not provided because students have no MAP results in at least one of the terms. The Growth Count is zero.

‡Growth Count provided reflects students with MAP results in both the Start and End terms. Observed Growth calculation is based on that student data.

Student Growth Summary Report

Aggregate by School

Term: Winter 2018-2019
District: SAU #41 (Hollis-Brookline SAU Office)

Norms Reference Data: 2015 Norms
Growth Comparison Period: Winter 2018 - Winter 2019
Weeks of Instruction: Start - 19 (Winter 2018)
 End - 16 (Winter 2019)

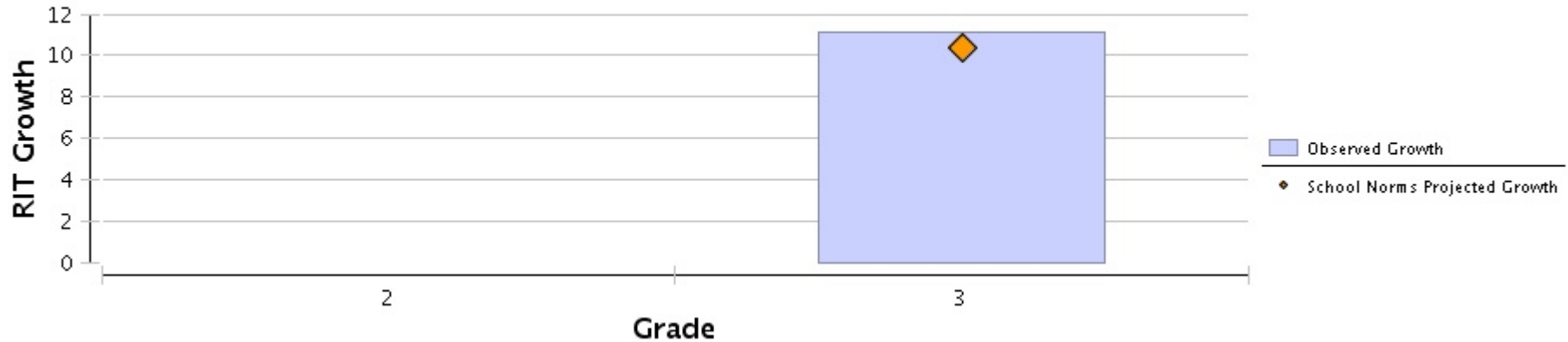
Grouping: None
Small Group Display: No

Richard Maghakian Memorial School

Reading

		Comparison Periods							Growth Evaluated Against							
		Winter 2018			Winter 2019			Growth		School Norms			Student Norms			
Grade (Winter 2019)	Growth Count‡	Mean RIT	SD	Percentile	Mean RIT	SD	Percentile	Observed Growth	Observed Growth SE	Projected Growth	School Conditional Growth Index	School Conditional Growth Percentile	Count with Projection	Count Met Projection	Percent Met Projection	Student Median Conditional Growth Percentile
2	0	**			**			**					**			
3	63	194.5	11.3	95	205.6	10.4	96	11.1	0.9	10.4	0.46	68	63	43	68	60

Reading



Explanatory Notes

** Calculations not provided because students have no MAP results in at least one of the terms. The Growth Count is zero.

‡Growth Count provided reflects students with MAP results in both the Start and End terms. Observed Growth calculation is based on that student data.

Student Growth Summary Report

Aggregate by School

Term: Winter 2018-2019
District: SAU #41 (Hollis-Brookline SAU Office)

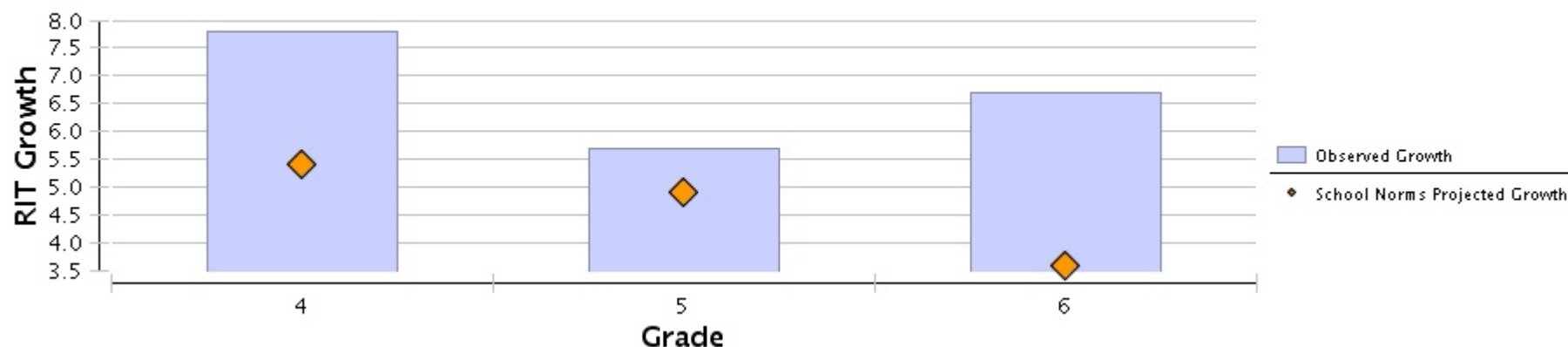
Norms Reference Data: 2015 Norms
Growth Comparison Period: Fall 2018 - Winter 2019
Weeks of Instruction: Start - 4 (Fall 2018)
 End - 16 (Winter 2019)
Grouping: None
Small Group Display: No

Captain Samuel Douglass Academy

Mathematics

Grade (Winter 2019)	Growth Count‡	Comparison Periods								Growth Evaluated Against						
		Fall 2018			Winter 2019			Growth		School Norms			Student Norms			
		Mean RIT	SD	Percentile	Mean RIT	SD	Percentile	Observed Growth	Observed Growth SE	Projected Growth	School Conditional Growth Index	School Conditional Growth Percentile	Count with Projection	Count Met Projection	Percent Met Projection	Student Median Conditional Growth Percentile
4	83	209.2	10.9	88	216.9	11.0	94	7.8	0.7	5.4	2.43	99	83	64	77	73
5	76	223.2	10.9	95	228.9	11.8	96	5.7	0.7	4.9	0.72	76	76	51	67	64
6	77	225.0	12.4	85	231.8	13.2	93	6.7	0.7	3.6	3.32	99	77	60	78	79

Mathematics



Explanatory Notes

‡Growth Count provided reflects students with MAP results in both the Start and End terms. Observed Growth calculation is based on that student data.

Student Growth Summary Report

Aggregate by School

Term: Winter 2018-2019
District: SAU #41 (Hollis-Brookline SAU Office)

Norms Reference Data: 2015 Norms
Growth Comparison Period: Fall 2018 - Winter 2019
Weeks of Instruction: Start - 4 (Fall 2018)
 End - 16 (Winter 2019)

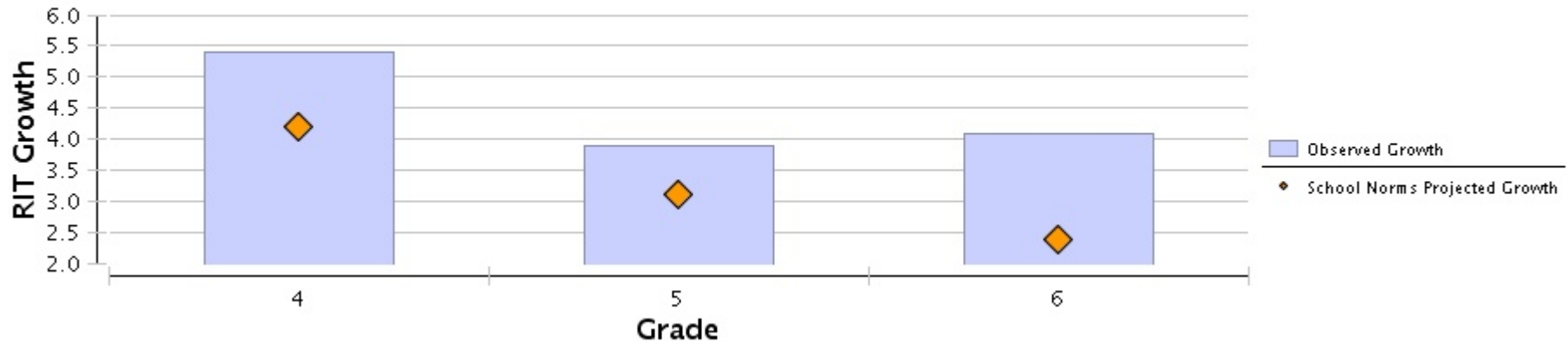
Grouping: None
Small Group Display: No

Captain Samuel Douglass Academy

Reading

Grade (Winter 2019)	Growth Count‡	Comparison Periods								Growth Evaluated Against						
		Fall 2018			Winter 2019			Growth		School Norms			Student Norms			
		Mean RIT	SD	Percentile	Mean RIT	SD	Percentile	Observed Growth	Observed Growth SE	Projected Growth	School Conditional Growth Index	School Conditional Growth Percentile	Count with Projection	Count Met Projection	Percent Met Projection	Student Median Conditional Growth Percentile
4	83	207.9	12.9	93	213.4	11.0	96	5.4	0.7	4.2	1.85	97	83	53	64	65
5	76	216.6	10.7	96	220.5	9.2	97	3.9	0.7	3.1	1.03	85	76	47	62	60
6	77	221.5	10.3	95	225.6	9.9	97	4.1	0.7	2.4	2.04	98	77	52	68	67

Reading



Explanatory Notes

‡Growth Count provided reflects students with MAP results in both the Start and End terms. Observed Growth calculation is based on that student data.



SAU41

Data Governance Plan

April, 2019

DRAFT

Contents

[Introduction](#)

[Data Governance Team](#)

[Purpose](#)

[Scope](#)

[Regulatory Compliance](#)

[Data User Compliance](#)

[Data Lifecycle](#)

[Identifying Need & Assessing Systems for District Requirements](#)

[New Systems](#)

[Review of Existing Systems](#)

[Acquisition and Creation](#)

[Management and Storage](#)

[Systems Security](#)

[Data Management](#)

[Data Classification and Inventory](#)

[Security/Protection](#)

[Risk Management](#)

[Security Logs](#)

[Physical Security Controls](#)

[Inventory Management](#)

[Virus, Malware, Spyware, Phishing and SPAM Protection](#)

[Electronic Access Security Controls](#)

[Securing Data at Rest and Transit](#)

[Usage and Dissemination](#)

[Data Storage and Transmission](#)

[Training](#)

[Archival and Destruction](#)

[District Data Destruction Processes](#)

[Asset Disposal](#)

[Critical Incident Response](#)

[Business Continuity](#)

[Disaster Recovery](#)

[Data Breach Response](#)

[Appendix A - Definitions](#)

[Appendix B - Laws, Statutory, and Regulatory Security Requirements](#)

[Appendix C - Digital Resource Acquisition and Use](#)

[Appendix D - Data Security Checklist](#)

[Appendix E - Data Classification Levels](#)

[Appendix F - Securing Data at Rest and Transit](#)

[Appendix G - Physical Security Controls](#)

[Appendix H - Asset Management](#)

[Appendix I - Virus, Malware, Spyware, Phishing and SPAM Protection](#)

[Appendix J - Account Management](#)

[Appendix K - Data Access Roles and Permissions](#)

[Appendix L - Password Security](#)

[Appendix M - Technology Disaster Recovery Plan](#)

[Appendix N - Data Breach Response Plan](#)

DRAFT

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.

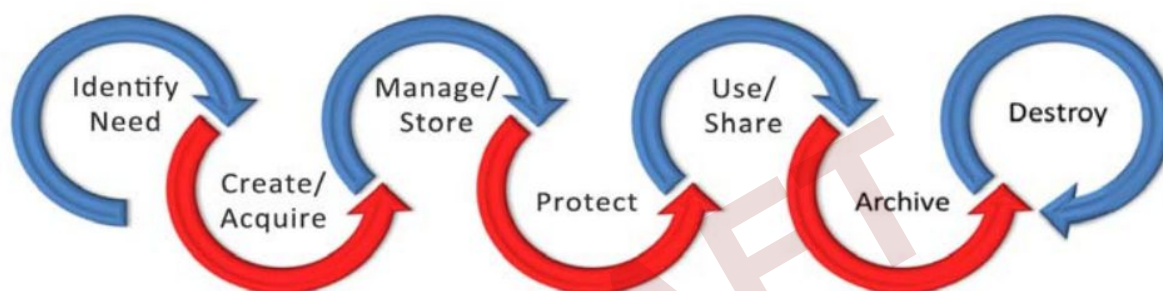
Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- 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.

DRAFT

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 (PHI). 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

DRAFT

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:
 - o kept on file at the District Office.
 - o accurate, up to date, and adequate.
 - o in compliance with all copyright laws and regulations.
 - o 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.

DRAFT

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.

DRAFT

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.

DRAFT

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

- Administrator
- Manager

Register Roles

- Administrators
- POS Cashier
- Manager

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

DRAFT

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.

DRAFT

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.

Brookline School District Expense Revenue Report

Brookline

FY19

THRU 04/09

<u>Expense</u>		<u>Annual</u>	<u>YTD</u>		<u>Q4</u>	
<u>Function</u>	<u>Description</u>	<u>Budget</u>	<u>Expense</u>	<u>Encumbered</u>	<u>Balance</u>	<u>REASON</u>
1100	Regular Education	2,703,240.87	1,760,511.70	943,308.25	(579.08)	
1200	Special Education	1,152,429.55	756,630.35	427,469.37	(31,670.17)	Unexpected SPED Students
2100	Student Support Services	608,418.48	458,279.14	163,913.76	(13,774.42)	Unexpected SPED students
2200	Instructional Staff Support	222,891.18	138,023.68	66,729.60	18,137.90	<PD not yet assigned
2300	School Board/SAU Assessment	364,677.00	258,948.25	61,557.91	44,170.84	<Includes \$50K for Contingency
2400	School Administration	460,399.16	353,944.39	94,822.42	11,632.35	
2600	Facilities	604,743.09	481,022.13	143,210.70	(19,489.74)	EE OT to cover for leave
2700	Transportation	443,000.00	325,291.97	122,326.49	(4,618.46)	Unexpected SPED students
2900	Benefits	2,220,826.67	1,474,386.07	724,803.39	21,637.21	Use of contractors saves on benefits
5100	Bonds	478,650.00	478,650.00	-	-	
5200	Transfers	420,000.00	-	420,000.00	-	
		9,679,276.00	6,485,687.68	3,168,141.89	25,446.43	
	FY18 Expense CarryOver	33,965.60	26,094.96	7,870.64	-	
		9,713,241.60	6,511,782.64	3,176,012.53	25,446.43	

Revenue

		<u>Budget</u>	<u>YTD</u>	<u>Expected</u>	<u>Balance</u>	
			<u>Revenue</u>			
1111	Local Property Tax	6,549,282.49	5,650,000.00	899,282.49	-	
1100, 1112, 1500, 1900	Local Impact Fees	5,000.00	17,034.16		(12,034.16)	Impact Fees
3110	Adequacy Aid Grant/Tax State	2,245,489.65	1,688,775.57	556,714.08	-	
3230	Catastrophic Aid	53,878.00	52,005.85		1,872.15	
3210	Building Aid	46,987.00	23,493.29	23,493.71	-	
21.3260	Food Service	2,100.00	2,077.23	-	22.77	
	Federal		-			
22.4300-4570	Grants	180,000.00	108,626.54	71,373.46	-	
21.4560	Food Service	40,500.00	21,619.52	18,880.48	-	
4570	Disabilities Program	-				
4580	Medicaid	19,025.00	16,965.54	2,059.46	-	
	Local		-			
314, 1317, 1322, 1990.01	Tuition	153,715.00	178,026.36	50,000.00	(74,311.36)	Higher Kindergarten Enrollment
1510, 1910, 1990, 3220	Other	65,182.00	68,915.49		(3,733.49)	
21.1600-1699	Food Service Sales	122,400.00	106,715.18	15,684.82	-	
	Less Contingency Fund (FY19)	50,000.00	-	50,000.00	-	
	Less Facilities Maintenance Fund (FY19)	50,000.00				
	Less Special Education Fund (FY19)	25,000.00	-	25,000.00	-	
	Fund Balance to Reduce Taxes (FY19)	70,716.86	-	70,716.86	-	
		9,679,276.00	7,934,254.73	1,783,205.36	(88,184.09)	
	Unreserved Fund Balance				\$ 113,631	
	Less Special Education Fund (FY20)				\$ 50,000	
	Less Facilities Maintenance Fund (FY20)				\$ 50,000	
	Less Contingency Fund (FY20)				\$ 25,000	
	Sub-Total				\$ (11,369)	

JH - ATTENDANCE, ABSENTEEISM AND TRUANCY

Category: Priority/Required by Law

Absences

The Board requires that school-aged children enrolled in the District attend school in accordance with all applicable state laws and Board policies. The educational program offered by the District is predicated upon the presence of the student and requires continuity of instruction and classroom participation in order for students to achieve academic standards and consistent educational progress.

Attendance shall be required of all students enrolled in the District during the days and hours that school is in session, except that the Principal may excuse a student for temporary absences when receiving satisfactory evidence of conditions or reasons that may reasonably cause the student's absence.

The Board considers the following to be excused absences:

1. Illness
2. Recovery from an accident
3. Required court attendance
4. Medical and dental appointments
5. Death in the immediate family
6. Observation or celebration of a bona fide religious holiday
7. Such other good cause as may be acceptable to the Principal or permitted by law

~~Any absence that has not been excused for any of these reasons will be considered an unexcused absence.~~

Any absence that has not been excused for any of these reasons will be considered an unexcused absence / truancy. More than 10 half days of unexcused absence per school year is considered habitual truancy.

Please note the following important attendance related procedural requirements:

- In the event of an illness, parents must call the school and inform the District of the student's illness and absence. For other absences, parents must provide written notice or a written excuse that states one of these reasons for non-attendance. The Principal may require parents to provide additional documentation in support of their written notice, including but not limited to doctor's notes, court documents, obituaries, or other documents supporting the claimed reason for non-attendance. A note from a medical provider is required when a student is absent for **5 or more** consecutive days due to illness. The note must contain the specific dates to be excused. These absences are unexcused until an excusal note is received.
- Up to **6 days** of vacation or educational opportunity may be considered excused each school year. In accordance with school board policy, a letter from parents in advance is required for approval.
- Student attendance records are reviewed regularly. In situations where students are experiencing multiple absences, intervention plans are put in place. Strategies to assist students with improving their attendance may include, but are not limited to: attendance alert letter, parent phone call and/or conference, request for documentation, consideration of the need for additional/alternate services, and a home visit, among other interventions.

If parents wish for their child to be absent for a reason not listed above, the parent must provide a written explanation of the reason for such absence, including why the student will be absent and for how long the student will be absent. The

Principal will make a determination as to whether the stated reason for the student's absence constitutes good cause and will notify the parents via telephone and writing of his/her decision. If the Principal determines that good cause does not exist, the parents may request a conference with the Principal to again explain the reasons for non-attendance. The Principal may then reconsider his initial determination. However, at this juncture, the Principal's decision shall be final.

Family Vacations/Educational Opportunities

Generally, absences other than for illness during the school year are discouraged. The school principal or his/her designee may, however, grant special approval of absence for family vacations, provided written approval is given in advance. Parents are asked to write a note to their child's teacher at least two weeks before the trip. This advance planning will allow the teacher enough time to work with parents and the student regarding homework completion.

Truancy

Truancy is defined as any unexcused absence from class or school. Any absence that has not been excused for any of the reasons listed above will be considered an unexcused absence.

Ten half-days of unexcused absence during a school year constitutes habitual truancy.

A half-day absence is defined as a student missing more two hours of instructional time and less than three and one-half hours of instructional time.

Any absence of more than three and one-half hours of instructional time shall be considered a full-day absence.

The Principal or Truant Officer is hereby designated as the District employee responsible for overseeing truancy issues.

Intervention Process to Address Truancy

The Principal shall ensure that the administrative guidelines on attendance properly address the matter of truancy by including a process that identifies students who are habitually truant, as defined above.

When the Principal identifies a student who is habitually truant or who is in danger of becoming habitually truant, he/she shall commence an intervention with the student, the student's parents, and other staff members as may be deemed necessary. The intervention shall include processes including, but not limited to:

1. Investigates the cause(s) of the student's truant behavior;
2. Considers, when appropriate, modification of his/her educational program to meet particular needs that may be causing the truancy;
3. Involves the parents in the development of a plan designed to reduce the truancy;
4. Seeks alternative disciplinary measures, but still retains the right to impose discipline in accordance with the District's policies and administrative guidelines on student discipline; and
- ~~5. Determination as to whether school record keeping practices and parental notification of the student's absences have an effect on the child's attendance.~~

Parental Involvement in Truancy Intervention

When a student reaches habitual truancy status or is in danger of reaching habitual truancy status, the Principal will send the student's parent a letter which includes:

1. A statement that the student has become or is in danger of becoming habitually truant;
2. A statement of the parent's responsibility to ensure that the student attends school; and
3. A request for a meeting between the parents and the Principal to discuss the student's truancy and to develop a plan for reducing the student's truancy.

Developing and Coordinating Strategies for Truancy Reduction

The Board encourages the administration to seek truancy-prevention and truancy-reduction strategies along the recommendations listed below. However, these guidelines shall be advisory only. The Superintendent is authorized to develop and utilize other means, guidelines and programs aimed at preventing and reducing truancy.

1. Coordinate truancy-prevention strategies based on the early identification of truancy, such as prompt notification of absences to parents.
2. Assist school staff to develop site attendance plans by providing development strategies, resources, and referral procedures.
3. Encourage and coordinate the adoption of attendance-incentive programs at school sites and in individual classrooms that reward and celebrate good attendance and significant improvements in attendance.

Parental Notification of Truancy Policy

~~Prior to adopting this policy, the Board will place the item on the agenda of a public school board meeting and will allow two weeks for public input as to the policy's provisions. Any public input shall be advisory only and final adoption as to the policy's provisions will remain solely with the Board.~~

~~Additionally, The Superintendent shall also ensure that this policy is included in or referenced in the student handbook. and is mailed to parents annually at the beginning of each school year.~~

~~NHSBA Note, September 2013: Due to legislative amendments to RSA 189:34, effective September 1, 2013, the only amendment to this Sample Policy is in Section "Intervention Process to Address Truancy", Paragraph #5.~~

Legal References:

RSA 189:34, Appointment

RSA 189:35-a, Truancy Defined

RSA 193:1, Duty of Parent; Compulsory Attendance by Pupil

RSA 193:7 Penalty

RSA 193:8, Notice Requirements

RSA 193:16 Bylaws as to Nonattendance

NH Code of Administrative Rules, Section Ed 306.04 (a)(1), Attendance and Absenteeism

NH Code of Administrative Rules, Section Ed 306.04 (c), Policy Relative to Attendance and Absenteeism

Reviewed: September 2013

Revised: July 1998, November 1999, February 2006, May 2008, September 2010

First Review: November 23, 2010

Second Review: December 21, 2010

Third Review: February 22, 2011

Adopted: December, 2011

First Review: March 27, 2019

Second Review: April 17, 2019