Brookline School Board - Jun 10 2026 Agenda

Wednesday, June 10, 2026 at 6:00 PM

Richard Maghakian Memorial School

Page

A. 6:00pm Call to Order

1. Agenda Adjustments
2. Consent Agenda 3

   FY26 Consent Agenda - Brookline - June (1).pdf
3. Approval of Minutes

B. 6:05pm Principal's Report

1. CSDA and RMMS reports 4

   June Principal Report 2026 (1).pdf
2. EOY Presentation 6

   School Board Presentation- June 2026.pdf

C. 6:15pm Public Hearing

1. Special Ed Trust 26

   BSD MEMO Spec. Ed. Trust 6.10.2026.pdf

D. 6:30pm Public Input

E. 7:00pm Discussion

1. CIP
2. Revenue and Expense 27

   BSD FY26 Expense & Revenue Report 6.4.2026.pdf
3. Data Governance Plan 29

   DGP Executive Summary June 2026.pdf

   SAU41 Data Governance Plan DRAFT 2026.pdf
4. Committee Updates

F. 7:15pm Deliberation

1. To see what action the Board will take regarding giving authority to the superintendent the authority to hire, etc...
2. To see what action the Board will take regarding the special education trust
3. To see what action the Board will take regarding the proposed policy memo 73

   6.10.26 BSB Policy Memo.pdf

   JICK (BSB) Pupil Safety and Violence Prevention - Bullying (1) (1).docx

   EBCA (BSD) Crisis Prevention and Emergency Response Plans (1).docx

   IMG (BSD) Animals in the Classroom (1) (2) (1).docx

   BEDB_ Agenda Preparation and Dissemination-Draft 5-31-26 (1) (1).docx

G. 7:45pm Non-Public

Motion to Enter RSA 91-A: 3II (a) Compensation and/or (c) reputation

H. 8:00pm Member Interest

I. 8:05pm Motion to Adjourn

School Administrative Unit #41
Hollis, Brookline & Hollis Brookline Cooperative School Districts
603 324 5999
4 Lund Lane, Hollis, NH 03049

June 2026

Nominations

Name	Position	Location	Lane/Step	Salary	Degree/Credentials

Resignations/Retirements

Name	Position	Location	Reason	Notes
Annie Oppelaar	Case Manager	RMMS	Resignation	

Brookline School Administrator's Report
June 10, 2026

Enrollment History

Year	September Enrollment	June Enrollment
16-17	552	567
17-18	550	550
18-19	574	573
19-20	577	580
20-21	572	583
21-22	587	591
22-23	580	589
23-24	583	582
24-25	554	563
25 - 26	554	564

RMMS Enrollment - 310
CSDA Enrollment - 254
Brookline Total Enrollment - 564

	PreK 3/4	K	1	2	3	4	5	6
Enrollment Total	26	76	69	78	61	91	84	79
Ed 306.12 Class Size		25	25	25	30	30	30	30
Divisor according to Policy IIB		17	17	20	20	23	23	23
Sections according to Policy IIB	12	4.47	4.05	3.9	3.05	3.96	3.61	3.39
Teacher/Class Size according to Policy IIB	14,, 12	15, 15,15, 15, 16	13,13,14, 14,15,	15,15,16, 16, 16	15,15,15, 16	22,22,23 24	20,21,21 22	19,20,20 20

May 28th– CSDA Innovation Stations
May 28th– CSDA Band & Chorus Concert
May 28th - PreK Seacoast Science Program
May 29th - Leaping Lizards visits Second Grade
May 29th-- Grade 6 Field Trip: America's Stonehenge
June 2nd - Field day
June 4th - Third grade visit to CSDA
June 4th - Preschool ends
June 4th-- HBHS Senior Walk Through
June 10th - Grade K visit to Friendly Farm
June 12th - Field Day
June 15th - Promotion Ceremony
June 16th - Last Day of School

Brookline Staffing Needs:
RMMS: 0.5 Paraeducators
CSDA: 5 Paraeducators
Brookline: School Psychologist

- **Please see our Year in Review Presentation**

Brookline
Year in Review

Mission:

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

Vision Statement:

"With our focus on the Whole Child, we foster capable, confident, lifelong learners who will serve as productive citizens in a global society. We are passionate about creating an environment that supports a love of learning, embraces active intellectual engagement and promotes high expectations for all."

RMMS Highlights

-01-

Environmental Science

Highlights:

Grade K - animals getting ready for winter, penguins and earthworms.

Grade 1 - oak trees, Arctic animals and animal classification.

Grade 2 - seed dispersal, erosion and pollinators

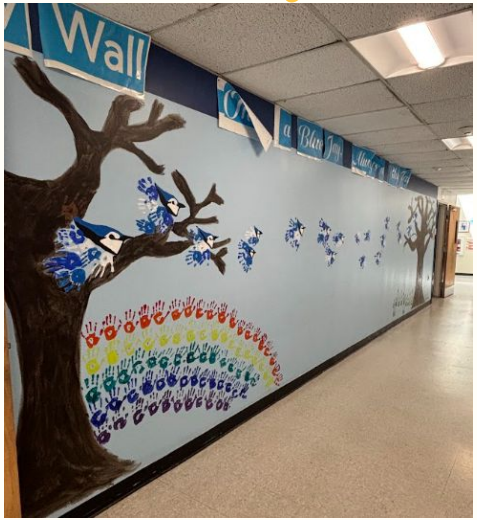
Grade 3 - evergreens, magnets and the food chain.

-02-

Amplify-CKLA

Highlights:

- Full implementation K-3
- Professional Development- onsite and virtual
- PLC Meetings-CKLA focus
- Cross Curricular Connections
- Culminating Activities

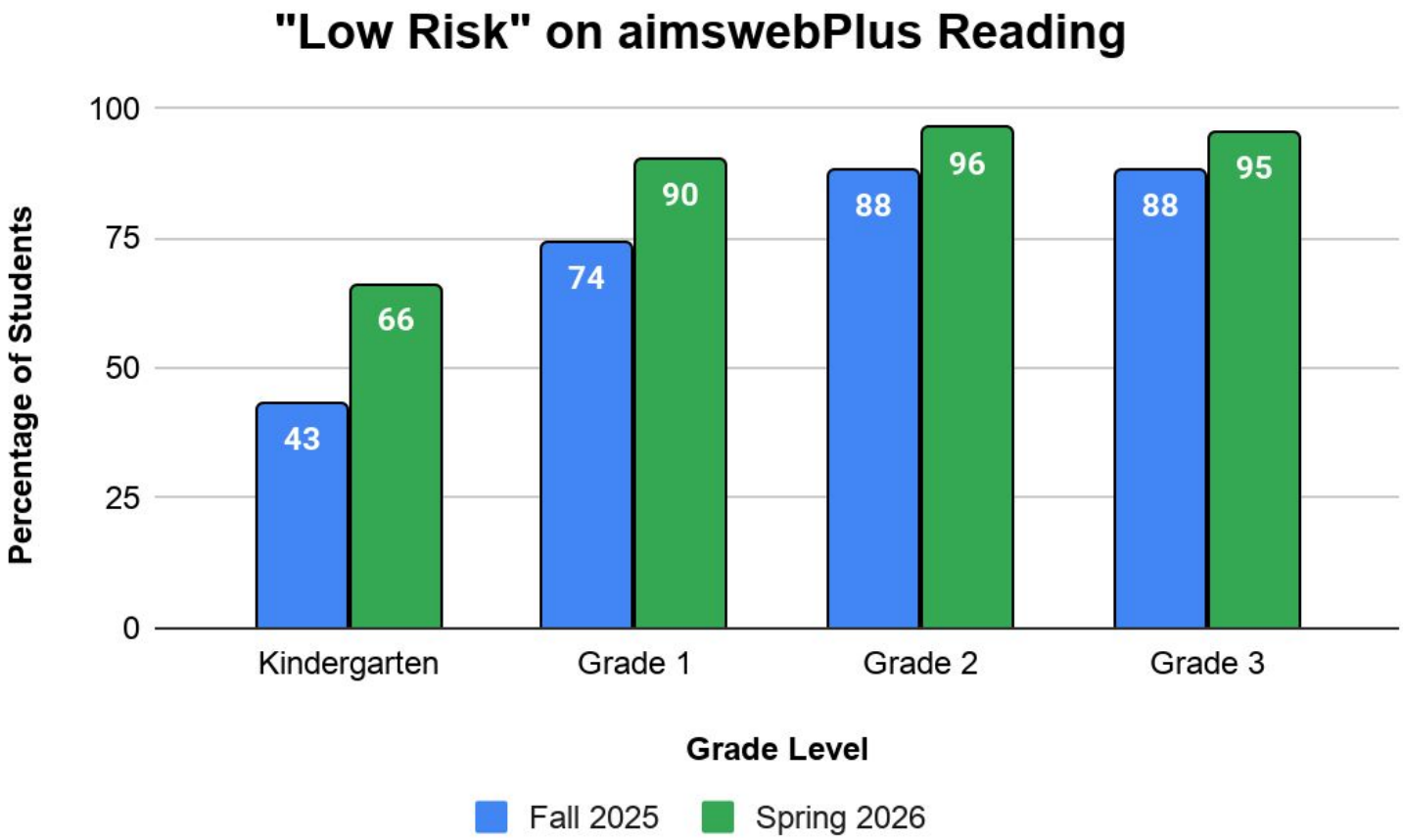


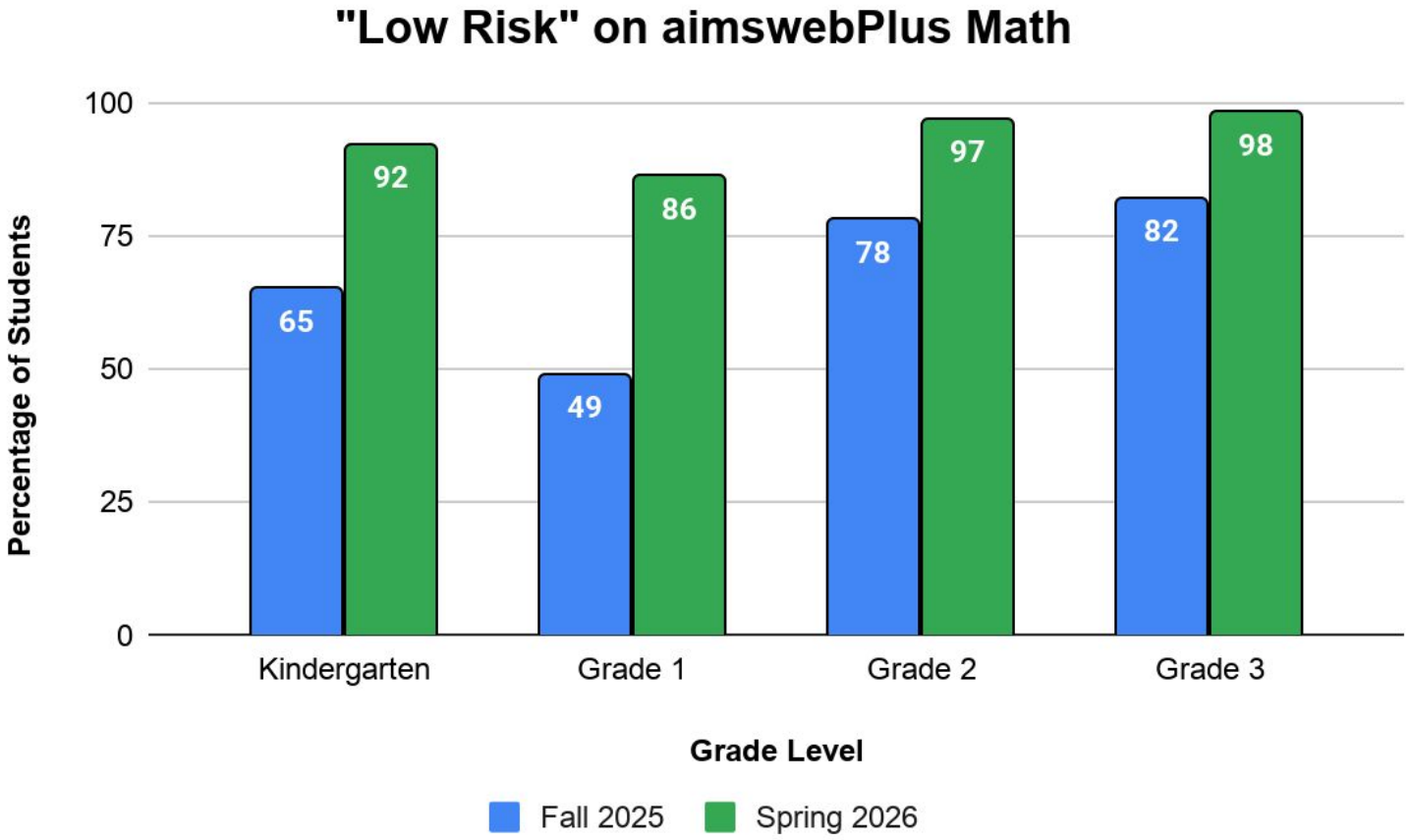
District Goals

Curriculum, Instruction & Assessment :

Refine our school-wide Multi-Tiered System of Supports (MTSS) to effectively address all academic subject areas and meet the diverse academic needs of all students.

- RMMS
  - Data & MTSS meetings
  - PLCs
    - Building Thinking Classrooms
    - Amplify CKLA
  - Cross-Curricular Connections
    - Environmental Science and Health


"Low Risk" on aimswebPlus Reading
Percentage of Students
100
75
50
25
0
43
66
74
90
88
96
88
95
Kindergarten
Grade 1
Grade 2
Grade 3
Grade Level
Fall 2025
Spring 2026


"Low Risk" on aimswebPlus Math
Percentage of Students
100
75
50
25
0
65
92
49
86
78
97
82
98
Kindergarten
Grade 1
Grade 2
Grade 3
Grade Level
Fall 2025
Spring 2026

District Goals

Student Well-being

Review and strengthen our school-wide Multi-Tiered System of Supports for Behavior (MTSS-B) to ensure consistent, effective teaching and reinforcement of behavior expectations and routines.

- RMMS
  - Blue Jay Recognition System (kindness, responsibility, respect, leadership, and perseverance)
  - Monthly birthday celebrations
  - Blue Jay t-shirts for all students and staff to wear during field trips and school-wide events.
  - School-Wide Way of the Jay weekly assemblies and skits in January, February, and May
  - Kindergarten Bootcamp with Mrs. H.
  - MTSS-B PLC meetings- September, October, November, January, March, and May

79% of students (245 out of 310) had 0 incidents, compared to 79% last year
92% of students (285 out of 310) had 1 or fewer incidents, compared to 91% last year
<1% of students had 15 or more incidents, compared to 3% last year

2025-2026	RMMS Incidents	Bus
September	25	9
October	35	22
November	13	9
December	22	5
January	30	5
February	20	2
March	24	3
April	27	4
May	16	3
June	5	0
Total	**217**	**62**

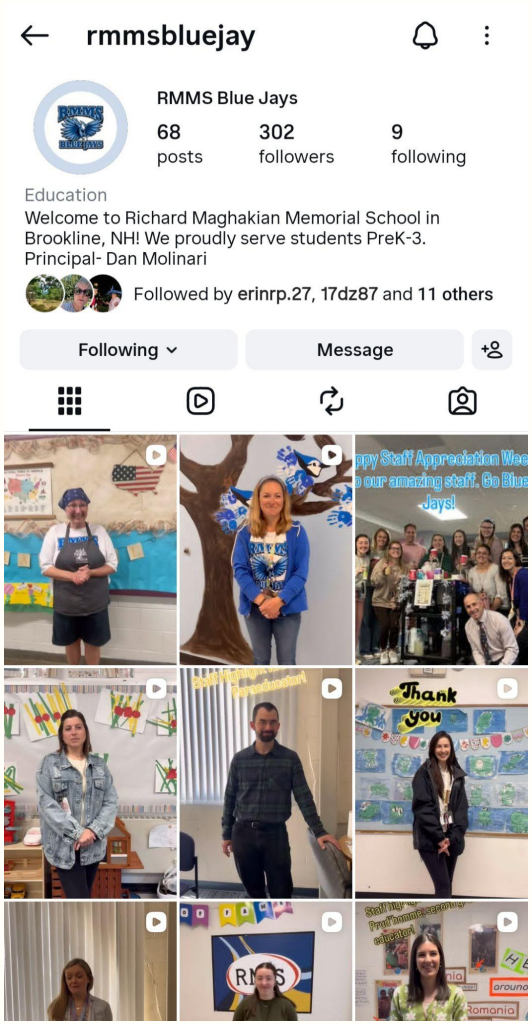
2024-2025	RMMS Incidents	Bus
September	44	9
October	32	6
November	18	11
December	13	10
January	22	8
February	25	1
March	63	8
April	28	6
May	34	9
June	8	6
Total	**287**	**75**

District Goals

Culture & Climate

The Brookline School District will review and refine lines of communication to students, staff, families, and the community in an effort to ensure its effectiveness.

- RMMS
  - Blue Jay T-Shirts
  - Once a Blue Jay, Always a Blue Jay - handprint wall
  - Instagram
  - ParentSquare


rmmsbluejay
RMMS Blue Jays
68 posts
302 followers
9 following
Education
Welcome to Richard Maghakian Memorial School in Brookline, NH! We proudly serve students PreK-3.
Principal- Dan Molinari
Followed by erinrp.27, 17dz87 and 11 others
Following
Message


Richard Maghakian Memorial School
Brookline School District | Grades PreK-3
603 673 4640
22 Milford Street, Brookline, NH 03033
May 29, 2026 | Volume 9, Issue 4
Important Dates
June 4th - Third grade visit to CSDA
June 5th - End of aimsweb Testing
June 10 - Kindergarten Field Trip to Friendly Farm
June 12 - Field Day (rain date June 15)
June 16th - Last Day of School, half day (Carpool begins at 11:15 a.m., Buses begin at 11:30 a.m.)
Please continue to scroll for Health Office Updates,
Community Happenings and more!

CSDA Highlights

-01-

Wolfpack Council, Student Murals & Wolfpack Leaders

We developed broad systems and structures that incorporate student voice. This includes a student council, student generated hallway murals, and implementation of a behavior program to develop student self-management

-02-

Foundational Instructional Work

In this first year of a multi-year initiative, we focused on 'how' we deliver instruction, ensuring we are teaching how the brain learns (specifically focusing on student turn & talk, as well as ensuring students understand learning objectives - the 'why' behind their learning)

-03-

Recess Revitalization

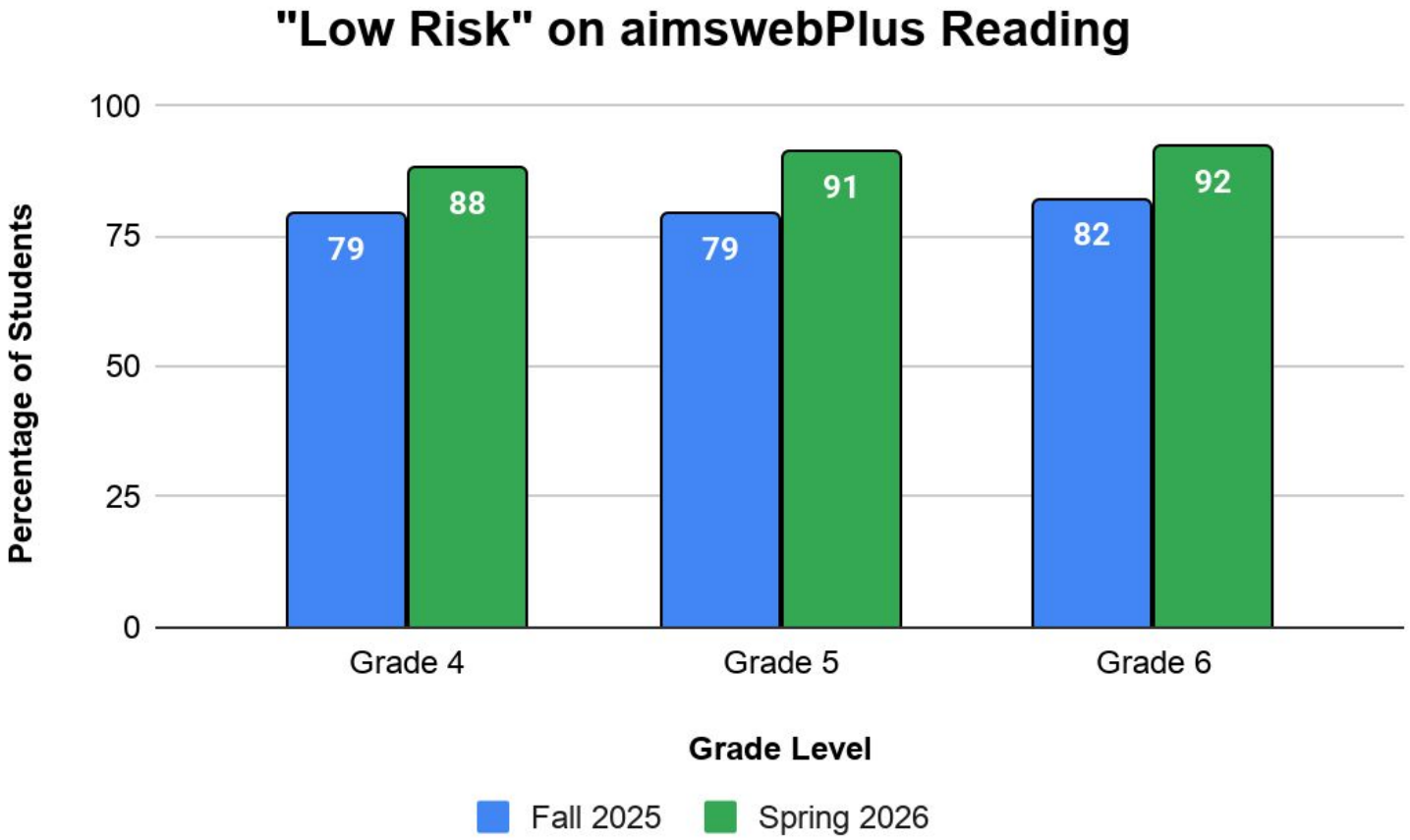
Adding music, real-time behavior redirections by supervising staff, & additional organized activities (wiffle ball, gaga ball, four square, wall-ball, football) we created a more structured, inclusive environment during the most social time of the school day.

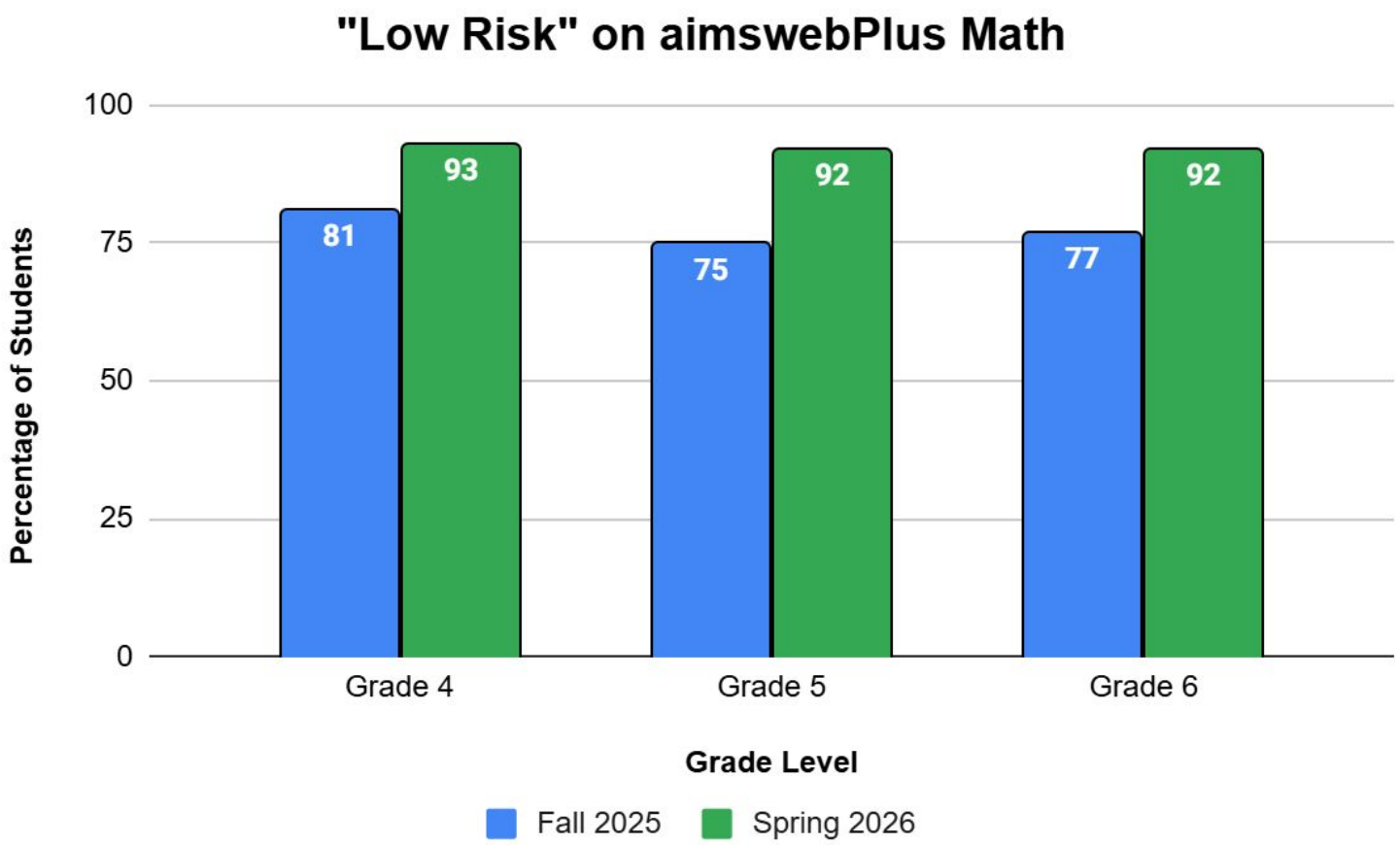
District Goals

Curriculum, Instruction & Assessment:

Refine our school-wide Multi-Tiered System of Supports (MTSS) to effectively address all academic subject areas and meet the diverse academic needs of all students.

- CSDA
  - Data & MTSS meetings
  - Ongoing Professional Development: Teaching How the Brain Learns
    - Turn & Talks; Learning Objectives


"Low Risk" on aimswebPlus Reading
Percentage of Students
100
75
50
25
0
79
88
79
91
82
92
Grade 4
Grade 5
Grade 6
Grade Level
Fall 2025
Spring 2026


"Low Risk" on aimswebPlus Math
100
75
50
25
0
Percentage of Students
81
93
75
92
77
92
Grade 4
Grade 5
Grade 6
Grade Level
Fall 2025
Spring 2026

District Goals

Student Well-being

Review and strengthen our school-wide Multi-Tiered System of Supports for Behavior (MTSS-B) to ensure consistent, effective teaching and reinforcement of behavior expectations and routines.

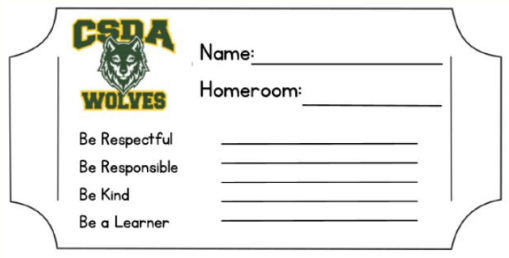
- CSDA
  - Wolf Pack Beliefs and Expectations
  - School Culture Blueprint

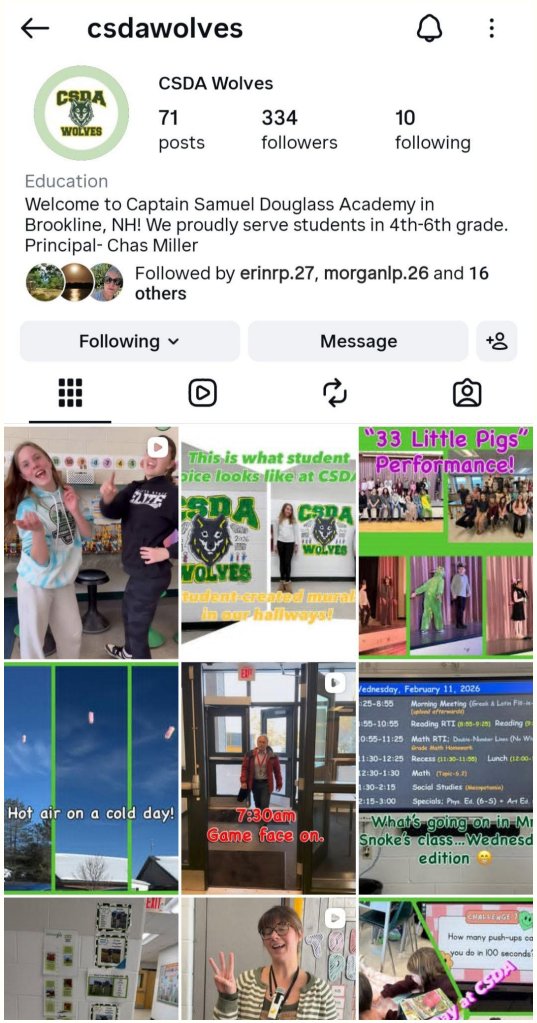
District Goals

Culture & Climate

The Brookline School District will review and refine lines of communication to students, staff, families, and the community in an effort to ensure its effectiveness.

- CSDA
  - Unity Day
  - Wolfpack Leaders
  - Pawsitive Pups
  - Wall Murals
  - Instagram
  - ParentSquare




csdawolves
CSDA Wolves
71 posts
334 followers
10 following
Education
Welcome to Captain Samuel Douglass Academy in Brookline, NH! We proudly serve students in 4th-6th grade.
Principal- Chas Miller
Followed by erinrp.27, morganlp.26 and 16 others
Following
Message
"33 Little Pigs" Performance!
Hot air on a cold day!
7:30am Game face on.


CSDA
WOLVES
Weekly Wolf Watch
May 29, 2026
Pack Updates

What we have done...

- Continue implementation and refinement of Responsive Classroom (all aspects) in all classrooms K-6
- Roll out of MTSS Interventionist and School Psychologist at both buildings
- Implementation of Amplify CKLA in K-3
- Continue implementation and refinement of Eureka Math2 in K-3
- Continue implementation and refinement of Amplify CKLA in grades 4 and 5, and Amplify ELA in grade 6.
- Refined delivery of and fidelity to enVision Mathematics and corresponding supports
- Professional development of Tier 1 Classroom Management
    - UNH; MTSS-B PLCs
- MTSS-B Tier 1 and 2 instruction and supports
- Creating regulation spaces at both buildings

Next Steps and Considerations:

- Continue MTSS-B Tier 1 instruction and support
- Targeted WIN Groups
- CKLA Culminating Cross-curricular activities

- CSDA - Intently connecting our SEL initiatives with our instructional routines to increase student engagement and student achievement
- CSDA - Implementing a strong PLC system where classroom teachers, interventionists, and specialists can meet on a regular basis to discuss teaching, learning, and social-emotional learning.

Thank you for your support!

School Administrative Unit #41
Hollis, Brookline & Hollis Brookline Cooperative School Districts
603 324 5999
4 Lund Lane, Hollis, NH 03049

Business Office Memo

To: Superintendent Bergskaug

From: Lance Flamino

Date: 6/10/2026

Subject: Special Education Expendable Trust

Use of Special Education Expendable Trust

As noted in the most recent expense and revenue report, the general fund is currently projected to end the fiscal year with an expense deficit of **($32,614)**. The primary factor contributing to this projected deficit is overspending within the special education budget, which currently has a negative balance of **($420,771)**.

These projections remain subject to change as the fiscal year concludes and final encumbrances and expenditures are reconciled.

Recommendations

To address any year end deficit attributable to Special Education expenditures, it is recommended that the board authorize the use of the Special Education Expendable Trust.

Given the uncertainty that remains in final year end balances, administration respectfully requests board authorization to expend up to **$75,000**, if necessary, from the Special Education Expendable Trust to balance year end expenses.

Brookline Special Education Expendable Trust Status

Current Balance:	$ 292,297
Purposed Authorization (not to Exceed):	$ 75,000
Resulting Balance (if fully utilized):	$ 217,297

Brookline School District
FY26
as of 6/4/2026

Expenses

Description	Budget	YTD Expense	Encumbered	Balance
Regular Education	$ 3,353,265	$ 2,543,405	$ 560,684	$ 249,176
Special Education	$ 2,391,834	$ 2,433,197	$ 379,408	$ (420,771)
Student Support Services	$ 992,880	$ 771,220	$ 162,775	$ 58,885
Instructional Staff Support	$ 353,093	$ 306,216	$ 64,013	$ (17,137)
School Board/SAU Assessment	$ 570,507	$ 494,053	$ 51,278	$ 25,176
School Administration	$ 729,218	$ 709,294	$ 42,079	$ (22,155)
Facilities	$ 938,804	$ 792,149	$ 84,477	$ 62,178
Transportation	$ 723,684	$ 575,155	$ 141,856	$ 6,673
Benefits	$ 2,868,593	$ 2,350,343	$ 500,471	$ 17,779
Site Development	$ 2	$ -	$ -	$ 2
Debt Service	$ 218,945	$ 211,365	$ -	$ 7,580
Transfers	$ 655,000	$ -	$ 655,000	$ -
TOTAL	**$ 13,795,825**	**$ 11,186,398**	**$ 2,642,041**	**$ (32,614)**
Plus FY25 Expense Carryover	$ 10,267	$ 9,696	$ 571	$ (0)
TOTAL FY25 + FY26	**$ 13,806,092**	**$ 11,196,094**	**$ 2,642,612**	**$ (32,614)**

Revenue

	Budget	YTD Revenue	Expected	IN EXCESS OF BUDGET
Local Property Tax	$ 10,174,585	$ 9,350,000	$ 824,585	$ (0)
Adequacy & SWEPT Grant	$ 2,834,440	$ 2,172,810	$ 661,630	$ 0
State				
Special Education Aid	$ 286,623	$ 326,542		$ 39,919
Other - State Aid	$ 3,225			$ (3,225)
State Funding	$ -			$ -
Food Service	$ 2,500	$ 3,028		$ 528
Federal				
Grants	$ 190,000	$ 103,226	$ 43,000	$ (43,774)
Food Service	$ 38,500	$ 35,717	$ 2,783	$ 0
Medicaid	$ 8,000	$ 34,642		$ 26,642
Local				
Tuition	$24,000	$ 51,389		$ 27,389
Impact Fees		$ 6,652		$ 6,652
Earnings on Investment	$ 20,000	$ 15,917	$ 4,083	$ (0)
Other	$ 1,000	$ 14,796		$ 13,796
Food Service Sales	$ 150,000	$ 185,165		$ 35,165
FY25 Expense Carryover	$ 10,267	$ 9,696	$ 571	$ 0
Less: Facilities Maint. Fund				$ -
Less: Special Education Fund	$ -			$ -
Fund Balance Adjustments	$ 248,144		$ 248,144	$ -
Less Retained Fund Balance	$ (185,192)		$ (185,192)	$ -
TOTAL REVENUE	**$ 13,806,092**	**$ 12,309,579**	**$ 1,599,604**	**$ 103,091**

Total Expense Balance	**$ (32,614)**
Plus Revenue Balance	**$ 103,091**
Less Txfr To Food Service Fund Balance	**$ (35,694)**
Unreserved Fund Balance Before Funding Items Below	**$ 34,783**

Anticipated Reductions to Unreserved Fund Balance

	Anticipated Needs for FY26
Maintenance Trust	
Retained Fund Balance	
Total Reductions	**$ -**

Projected Fund Balance	**$ 34,783**

* A negative balance here at year-end would require a special meeting with taxpayers

Explanation of budget balances on current expense report

6/3/2026

Function	Description	Current Balance	Notes
1100	**Regular Education**	$ 249,176	Unfilled positions
1200	**Special Education**	$ (420,771)	Contracted staffing
2100	**Student Support Services**	$ 58,885	Unfilled Psych position, offset in contracted staffing
2200	**Instructional Staff Support**	$ (17,137)	Several small expected overages
2300	**chool Board/SAU Assessment**	$ 25,176	Less legal services
2400	**School Administration**	$ (22,155)	New Admin hired/increased salaries/IT services
2600	**Facilities**	$ 62,178	Savings with oil and propane, offset snow removal overages
2700	**Transportation**	$ 6,673	small savings in transportation
2900	**Benefits**	$ 17,779	Unfilled positions and choice changes
4000	**Site development**	$ 2	
5100	**Debt Service**	$ 7,580	Estimated higher Interest for new lease
5200	**Transfers**	$ -	
		$ (32,614)	

General explanation of what is included in each account category

Function	Description	Includes
1100	Regular Education	Teacher salaries and teaching materials
1200	Special Education	Teacher salaries, teaching materials, ESY, out-of-district tuition
2100	Student Support Services	Guidance, nurse, psychologist, OT, teaching/testing supplies, contracted services
2200	Instructional Staff Support	Professional development, librarian, library supplies, computer equipment
2300	School Board/Assessment	Assessment, school board expense, annual meeting expense, legal expense
2400	School Administration	Administrator & secretarial salaries, copiers, telephone, hardware/software support contracts, site licensing, consulting, network services, office supplies
2600	Facilities	Custodial/maintenance salaries, snow plowing, mowing, building repairs, heating oil, electric, janitorial supplies, property/liability insurance
2700	Transportation	Bus transportation, fuel
2900	Benefits	Health and dental insurance, taxes, NHRS, Life/LTD, workers comp & unemployment
4000	Site Improvement	Site improvements including architectural fees
5100	Bonds	Principal and interest payments on bonds
5200	Transfers	expense

School Administrative Unit #41
Hollis, Brookline & Hollis Brookline Cooperative School Districts
603 324 5999
4 Lund Lane, Hollis, NH 03049

May 26, 2026
To: Superintendent Bergskaug
From: Data Governance Team
Re: Proposed Changes to the Data Governance Plan

The SAU41 Data Governance Team presents the following summarized changes to the SAU41 Data Governance Plan for Board and Superintendent acknowledgement:

Maintenance

1. Edits to reflect the correct members of the Team and their associated titles
2. Mainstreaming formatting across the file
3. Updating and correcting hyperlinks

Content

1. Rephrasing or removing language referring to policies not adopted by or applicable to the SAU41 School Boards and District
2. Updating practices regarding Google Suite and account disposal/ maintenance (page 12)

SAU41

Data Governance Plan

April 2026

Contents

Introduction

School Administrative Unit 41 (SAU41) also referred to as the District, 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 of Curriculum, Business Administrator, Director of Technology, and the Compliance and Communication Specialist. ~~Systems Administrator~~. Members of the Data Governance Team will act as data stewards for all data under their direction. The Director of Technology, and Systems Administrator 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 providing a wide range of technologies for a well-rounded education, in order to enhance 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 schools in 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 policies, 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. These policies apply to all forms of SAU41 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.
- 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.

The terms "data" and "information" are used separately, together, and interchangeably throughout the policies; the intent is the same.

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, to include but not limited to: EH (Data Management), EHAB (Data Governance and Security), EHB (Data/Records Retention), EHB-R, (Records Retention Schedule), GBEF (Employee Use of District-Issued Computers, Devices and the Internet), GBEBD (Social Media and Acceptable Use), GBEF-R (Employee Computer/Device and Internet Responsible Use Rules), JICJ (Communication Devices), (JICL (Student Use of Computers, Devices and the Internet), ~~JICL-R (Student Technology Responsible Use)~~ and all policies, procedures, and resources as outlined within this Data Governance Plan and School Board Policies.

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, District-owned Cloud storage, 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), or secure pathway. 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 up to and including termination. Volunteers may be excluded from providing services to the district. The District will end business relationships with any contractor who fails to follow the law, district policies or procedures, or the confidentiality provisions of any contract. In addition, the District reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of 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 or intended 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.

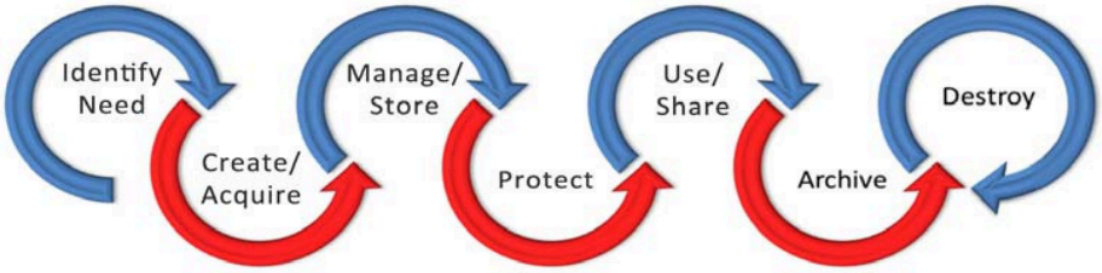
• Installation or use of unlicensed software or software not approved for district systems.

• 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 webpages, to ensure that all new resources meet business and/or instructional needs as well as security requirements.

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

All new resources shall be properly evaluated against the criteria identified in Appendix C. A current list of all vetted and approved software systems, tools and applications is published on SAU41s Technology webpage.

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. 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 the intended purpose.

Acquisition and Creation

Staff shall complete an online request form (located on the District website's Staff Only Area) for any new digital tool or resource (see Appendix C: Webtools 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 Webtools Request Form, staff should speak with their building Technology Integrator or Administrator to evaluate the site's content, use, and funding source, if applicable. No new digital tool/resource may be used until it has been vetted and approved by the DGT.
- 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, system access will only be given on an as-needed basis as determined by the ISOs for a predetermined length of time. 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. 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.

Multi-factor authentication is required for all staff Google Accounts. Additional security measures will be put in place as needed and determined by District Technology staff.

Security Logs

SAU41 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 closets are housed in secure locations. Access authorization is assigned through the Director of Technology. 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).

Technology systems shall be disposed of or moved according to the appropriate procedures (see Appendix H: Asset Management).

Inventory Management

SAU41 shall maintain a process for inventory control in accordance with 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

SAU41 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 filtering software. 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. This information will only be disclosed to authorized contractors or agents who need access to the information to provide services to one or more districts 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 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.

Educational and Facilities Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by the Business Administrator. All contractors doing business on district premises must comply with policy GBCD. 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

SAU41 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

Vendor or staff access into the District's network from outside the SAU41 network 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 SAU41's network.

Securing Data at Rest and Transit

SAU41 data security applies to all forms of data, including data stored on devices, data in transit and data stored on additional resources. Regular transmission of student data to internal and external services is managed by the technology department using secure data delivery methods.

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 SAU41'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, including, but not limited to Employee and Student Technology Usage (GBEF, GBEF-R, JICL, JICL-R), Data Governance and Security (EHAB), and Student Records (JRA~~, JRA-R~~).

SAU41 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 device will be provided with approved options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data locally and/or in the cloud. It is important to note that this data is not a part of SAU41's continuity plan, and thus will not be backed up by SAU41's backup solution.

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 SAU41 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

SAU41 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 SAU and 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

SAU41 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 EHAB ~~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

SAU41 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

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 based on when information is available, given that some systems are internal and others are external (cloud based). 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 incidents. 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 or unauthorized acquisition of 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. Per GBEBD-R, SAU41 is the owner of messages, documents and media created within the District's network. The "data" 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 they are 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, Chromebook, mobile device, printing and/or scanning device, network appliance/equipment, AV equipment, server, internal or external storage, communication device or any other current or future electronic or technological device, whether hosted by the district or provider.

Security Incident: An event that 1) actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits, or 2) constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

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

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

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

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

Appendix B - Laws, Statutory, and Regulatory Security Requirements

CIPA: The Children's Internet Protection Act was enacted by Congress to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies shall include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they shall provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

COPPA: The Children's Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information.
https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy

FERPA: The Family Educational Rights and Privacy Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

HIPAA: The Health Insurance Portability and Accountability Act applies to organizations that transmit or store Protected Health Information (PII). It is a broad standard that was originally intended to combat waste, fraud, and abuse in health care delivery and health insurance, but is now used to measure and improve the security of health information as well.
https://www.hhs.gov/hipaa/index.html

IDEA: The Individuals with Disabilities in Education Act (IDEA) is a law that makes available a free appropriate public education to eligible children with disabilities throughout the nation and ensures special education and related services to those children.
https://sites.ed.gov/idea/

PCI DSS: The Payment Card Industry Data Security Standard was created by a consortium of payment brands including American Express, Discover, MasterCard, and Visa. It covers the management of payment card data and is relevant for any organization that accepts credit card payments. www.pcisecuritystandards.org

PPRA: The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.
https://studentprivacy.ed.gov/topic/protection-pupil-rights-amendment-ppra

New Hampshire State RSA 189:65-189:68: Student and Teacher Information Protection and Privacy as defined by the following sections:

- NH RSA 189:65 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-65.htm) Definitions
- NH RSA 189:66 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-66.htm) Data Inventory and Policies Publication
- NH RSA 189:67 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-67.htm) Limits on Disclosure of Information
- NH 189:68 (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68.htm) Student Privacy
- NH RSA 189:68-a (http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68-a.htm) Student Online Personal Information

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

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

- NH RSA 359-C:19 (http://www.gencourt.state.nh.us/rsa/html/SAU41i/359-c/359-c-19.htm) Notice of Security Breach - Definitions
- NH RSA 359-C:20 (http://www.gencourt.state.nh.us/rsa/html/SAU41i/359-c/359-c-20.htm) Notice of Security Breach Required
- NH RSA 359-C:21 (http://www.gencourt.state.nh.us/rsa/html/SAU41i/359-c/359-c-21.htm) Notice of Security Breach Violation

Appendix C - Digital Resource Acquisition and Use

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

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

New Resource Acquisition

Staff are required to complete steps outlined under the SAU41 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 SAU41. All staff must adhere to the following guidelines regarding digital resource acquisition:

- Contracts (including renewals) 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. 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 SAU41 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:

- Curricular value
- NH Data Privacy Agreement
- Impact on technology environment including storage and bandwidth
- Impact on staff resources
- 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 risks, 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 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 devices owned by SAU41 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 SAU41 resources are to be used.
- District software licenses will be:
    - o kept on file at SAU41.
    - 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 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

□ Data Privacy Agreement,

□ 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 the District, its staff, parents, students or other stakeholders. Decisions about the provision of access to this information shall always be cleared through the data manager and/or ISO.

Internal Information

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

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

Directory Information

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

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

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

Public Information

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

This information may be disclosed outside of the district.

Appendix F - Securing Data at Rest and Transit

All staff and students that log into a district owned device 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.

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, when appropriate and feasible..

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 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 Cloud storage providers. 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,-administrator, technology staff member.
- 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 or technology staff member.

External Storage Devices

The term “External Storage Devices” is used to define all portable storage devices (including USB drives, 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 removed.
- 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 as 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 the 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 the individual making payment. If the individual is not able to directly input the payment, designated staff may gain verbal approval for the payment process either in person or via phone (after identification is verified). If verbal payment information is received, that information must be entered directly into the payment system and not written down during the process.

Appendix G - Physical Security Controls

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 server room shall afford reasonable 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, tablet, interactive flat panel, 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 SAU41 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, tablets, interactive flat panel, classroom audio system, 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
- Saleable value

The Director of Technology shall approve disposals of any district technology asset.

Methods of Disposal

Once equipment has been designated and approved for disposal (does not have saleable 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, track pads, memory). In addition, systems may contain Personally Identifiable Information (PII), Confidential, or Internal Information. Systems shall be wiped clean of this information prior to leaving the school district.

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

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

Donation/Gift

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

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

SAU41 School District desktops, laptops, Chromebooks, 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. SAU41 has adopted protections to prevent students and staff from installing third-party software.

Internet Filtering

To balance student learning resources and application use with student safety and network security, Internet traffic from all devices on the individual school's network is routed through a 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

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 a 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 Director of Technology.

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 accounts to be disabled at once, preventing any further access to district resources.
- In the event of resignation, HR will notify the Technology Department indicating the termination date. Accounts are 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.

Students

Are created upon completion of required enrollment forms and/or the beginning of the school year, as applicable.

Contactors

Approved contractor accounts are created based on role/need.

Local/Domain Administrator Access

Only members of the 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 SAU41 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 the SAU41 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, BA, and/or the ISOs. All contractors doing business on district premises must also pass a background check or employ other security measures that are defined by SAU41. Account access, when needed, will be set up by the Technology Department.

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

Staff demographics 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
- Staff type/position
- SAU41 email address
- Primary phone number

Access accounts for the SAU41's SIS are set up based on staff role/position, building and required access to student data and are assigned by the Director of Technology. 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 and role-based permissions.. Security groups control access to certain data sets such as attendance, demographic data, grades, health records, discipline etc. Additional page level permissions are assigned to the security groups. Administrative accounts log into the SIS Admin Portal.

SIS Security Groups*

- Administrator
- Athletics
- Counselor
- Technology Staff
- Office Staff
- Principal
- Registrar
- Nurse
- Secretary II
- 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
- Administrators
- HR Staff
- Maintenance
- Spec Ed Coordinator
- Spec Ed Secretary
- Sr. Secretary

* A complete list of permissions is kept on file in the Business Office.

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 to accounts in NHSEIS is maintained by the Director of Student 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

Food Services System

SAU41 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

Software Application Roles	**Register Roles**
• Administrator	• Administrators
• Manager	• POS Cashier
	• Manager

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

Appendix L - Account Security

The District requires the use of strictly controlled passwords and multi-factor authentication 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.
- New users will have a set period of time to enable multi-factor authentication on their accounts.
- 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 technology department staff 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 Lightweight Directory Access Protocol (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 must not contain usernames.
- District passwords should never be used 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 a 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:; Director of Technology, Network Manager, Database Manager, ~~Systems Administrator~~, Assistant Superintendent of Curriculum, 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

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

Deactivation

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

Evaluation

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

Appendix N - Cyber Incident Response Plan

Objectives

SAU41's Cyber Incident Response Plan is on file.

The purpose of the Cyber Incident Response Plan (CIRP) is to enable SAU41 (SAU41) to respond effectively and efficiently to an actual or suspected ~~data breach~~ incident involving unauthorized disclosure of confidential district information and/or other significant cybersecurity events. The objectives of the CIRP are:

- Convene the Incident Response Team (IRT) as necessary.
- Validate and contain the incident.
- Analyze the incident to determine scope and composition.
- Minimize impact to the staff and students after an incident has occurred.
- Notification of relevant parties.

Planning Assumptions

The following planning assumptions were used in the development of SAU41'sCIRP:

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

Cyber Incident Response Team

SAU41 has appointed the following people to the Cyber Incident Response Team (CIRT): Director of Technology, Systems Administrator, Assistant Superintendent, and Business Administrator.

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

- Determine the nature of the incident 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.
- Coordinate with the Superintendent to ensure communication with district staff and or parents as deemed appropriate.
- Oversight of the CIRP implementation and incident resolution.
- Allocate and manage technology staff resources during the event.
- Work with vendors, 3rd party providers, manufacturers, legal counsel, district risk management provider, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Oversight of CIRP implementation debrief with Data Governance Team.

Activation

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

- An incident has occurred and affects the district itself. A cyber incident 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 incident response and reporting process will be documented according to state and federal requirements. The Director of Technology, Systems Administrator will work with the Superintendent to dispense and coordinate the notification and public message of the incident.

Notification

The following groups will be notified in the event the plan has been activated, as deemed necessary per the scope of the incident:

- Legal counsel
- Risk management provider
- State and Federal agencies
- Law Enforcement
- Superintendent
- School Boards
- 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
- Written Notice
- Phone/SMS

The CIRP 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 CIRP team has the following processes in place to address the incident 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 an incident has been validated. The IRT will be comprised of the Director of Technology, Systems Administrator 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 incident, ongoing, active, or incident. For an active and ongoing incident, 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 applicable outside agencies to determine the scope and composition of the incident, secure sensitive data, mitigate the damage that may arise from the incident and determine the root cause(s) of the incident to devise mitigating strategies and prevent future occurrences.

• An outside party may be hired to conduct the forensic investigation of the ~~breach~~ incident. 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 IRT, legal counsel and the Superintendent 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 incident, such a determination shall be documented in writing and filed at the Superintendent's office.

Deactivation

The IRT will deactivate the plan once the incident has been fully contained.

Evaluation

Once the incident has been mitigated an internal evaluation of the SAU41's CIRP response will be conducted. The IRT will review the incident 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 CIRP and other emergency response plans as appropriate. Information security training programs will be modified to include countermeasures to mitigate and remediate previous incidents so that past incidents do not recur. The reports and incident review will be filed with all evidence of the incident.

Adoption History

Adopted: 2019

Re- Adopted: 2019

School Administrative Unit #41
Hollis, Brookline & Hollis Brookline Cooperative School Districts
603 324 5999
4 Lund Lane, Hollis, NH 03049

To: Superintendent Bergskaug
From: BSB Policy Committee
RE: Policy Recommendations
Date: June 1, 2026

The Brookline Policy Committee makes the following policy recommendations for the June 10th, 2026 Brookline School Board meeting:

Present for a 3rd read and adopt with no changes:

1. JICK: Pupil Safety and Violence Prevention

Present for a 2nd read and adopt with no changes:

1. EBCA: Crisis Prevention and Emergency Response Plans
2. IMG: Animals in the Classroom

Present for a 2nd read with major changes:

1. BEDB: Agenda Preparation and Dissemination

PUPIL SAFETY AND VIOLENCE PREVENTION - BULLYING

Category: Priority/Required by Law *See also JBAA, JIC, JICD, IHBA*

A. **Purpose and Intent:** The Brookline School District is committed to providing a safe and respectful learning environment for all students. Through education, prevention, and consistent enforcement, we aim to eliminate bullying and promote positive peer relationships for all of our students.

1. Prohibition of Bullying or Cyberbullying of a Student - RSA 193-F:4, II(a): This policy is intended to comply with and implement RSA 193-F. Bullying, in any form—whether physical, verbal, social, or cyber—is strictly prohibited and will not be tolerated. This policy defines bullying and related conduct, and establishes clear procedures for reporting, investigating, and responding to incidents.

2. Protection of all School Aged Children - RSA 193-F:4, II(c): This policy shall apply to all students and school-aged persons on school district grounds and participating in school district functions, whether or not such school-aged person is a student within the District and regardless of their status under the law. District staff will coordinate with staff from other districts, if an allegation of bullying involves a student who is not a resident of the District.

3. Prohibition of Retaliation and False Accusations - RSA 193-F:4, II(b): This policy prohibits retaliation or false accusations against a victim, witness, or anyone else who, in good faith, provides information about an act of bullying or cyberbullying. An unsubstantiated allegation of bullying, without more, will not constitute a false accusation against an alleged perpetrator.

B. Definitions (RSA 193-F:3)

1. Bullying: Bullying is hereby defined as a single significant incident or a pattern of incidents involving a written, verbal, or electronic communication, or a physical act or gesture, or any combination thereof, directed at another pupil which:

a. Physically harms a pupil or damages the pupil's property;

b. Causes emotional distress to a pupil;

c. Interferes with a pupil's educational opportunities;

d. Creates a hostile educational environment; or

e. Substantially disrupts the orderly operation of the school and

f. Either occurs on, is delivered to, school property or a school-sponsored activity or event on or off school property; or occurs off of school property or outside a school-sponsored activity or event, if the conduct interferes with a student's educational opportunities or substantially disrupts the orderly operations of the school or any school-sponsored activity or event.

Bullying shall include actions motivated by an imbalance of power based on a pupil's actual or perceived personal characteristics, behaviors, or beliefs, or motivated by the pupil's association with another person and based on the other person's characteristics, behaviors, or beliefs.

As used throughout this or other Board policies, and unless the context indicates otherwise, the term "bullying" as used in this policy will include cyberbullying.

2. "Cyberbullying" is defined as any conduct defined as "bullying" in this policy that is undertaken through the use of electronic devices. For purposes of this policy, any references to the term bullying shall include cyberbullying.
3. "Electronic devices" includes, but is not limited to, telephones, cellular or smartphones, computers, pagers, or any other device which is used for or can transmit: voice calls or messages; electronic mail; text/instant or other verbal messaging; images or videos; and websites.

4. "Parent" means a person who has legal custody of a minor child as a natural or adoptive parent, as a legal guardian, or who is functioning in a parental role if the actual parent or guardian is absent from the child's daily life. Additionally, "parent" may include students who have been emancipated, either by age or legal process. The term "parent", shall not, however, include a parent as to whom the parent-child relationship has been terminated by judicial decree or voluntary relinquishment.

5. "Perpetrator" means a student who engages in bullying or cyberbullying.

6. "Principal" shall mean and include the building Principal or other senior building administrator of a school, as well as any qualified person appointed by the Principal to carry out all or some Principal functions as described in this policy. References to "Principal" throughout this policy refer to the Principal or designee.

7. "Retaliation" means and includes such conduct as intimidation, threats, coercion, harassment, or discrimination in response to (or in an effort to prevent) a victim, alleged victim, witness or other person, who in good faith provides information about an act or conduct that the person providing the information believes is bullying or cyberbullying.

8. "School property" means all real property and all physical plant and equipment used for school purposes, including public or private school buses or vans.

9. "Staff" means and includes all district, school or SAU employees, designated volunteers (as defined in Board policy GBCD), or other volunteers who are regularly on school property, or who have significant contact with students, and any employees of a company under contract to the District or SAU and who have significant contact with students.

10. "Student" shall have the same meaning as "pupil" as used in RSA 193-F and this or any other Board policy.

11. "Superintendent" means the Superintendent (Senior Education Official) or other person designated by the Superintendent to carry out all or some Superintendent functions as described in this policy. References to "Superintendent" throughout this policy refer to the Superintendent or designee.

12. "Victim" means a student against whom bullying or cyberbullying has been perpetrated.

C. Retaliation - RSA 193-F:4, II(b). Retaliation or false accusations related to bullying or cyberbullying shall be deemed a violation of this policy, and students engaging in retaliation or making false accusations may be subject to disciplinary action. Upon receiving any report of bullying or cyberbullying, the Principal will immediately assess the need to develop a plan or take steps to protect the alleged victim or any witnesses against retaliation. The same assessment shall be made at any point upon a report of retaliation or false accusations made during or after a bullying/cyberbullying investigation.

Reports of retaliation or false accusations relating to a bullying/cyberbullying report may be made in the same manner as for reports of bullying/cyberbullying as provided in this policy.

Investigations, and responses (i.e., interventions, supportive measures, disciplinary consequences) to reports of retaliation or false accusations may be made as provided in the same manner as provided in the applicable sections below for reports or incidents of bullying/cyberbullying, or in accordance with procedures and provisions set forth in the student handbook

D. Procedures for Reporting Bullying, Cyberbullying, Retaliation or False Accusations - RSA 193-F:4, II(f). At each school, the Principal is responsible for receiving reports or complaints of bullying or cyberbullying.

1. Student Reporting: Any student who believes he or she has been the victim of bullying/cyberbullying, retaliation, or false accusations should report the alleged acts immediately to the Principal, or to a school district employee or volunteer that the student feels more comfortable making the report.

2. Staff Reporting: Any school employee or volunteer who receives a report of, witnesses, or has knowledge or belief that bullying/cyberbullying or retaliation may have occurred, shall inform the Principal as soon as possible, but no later than the end of that school day.

3. Parent Reporting: Parents and other adults are also encouraged to report any concerns about possible bullying/cyberbullying or retaliation of students to the Principal.

4. Report Forms: The administration may develop student reporting forms to assist students and staff in filing such reports. An investigation shall still proceed even if a student is reluctant to fill out the designated form and chooses not to do so.

5. Anonymous Reports: The Principal may develop a system or method for receiving anonymous reports of bullying within the building. Although students, parents, volunteers and visitors may report anonymously, an investigation based upon such reports may by necessity be incomplete. More significantly, formal disciplinary action may not be based solely on an anonymous report, and, likewise, other remedial or supportive measures may require some form of evidentiary verification.

E. Actions Upon Receipt of Report of Bullying or Cyberbullying

1. Receipt of Report: Upon receipt of a report of bullying, the Principal shall commence an investigation consistent with the provisions of Section F of this policy and shall assess:

a. the need for a plan to protect students against retaliation,

b. whether the conduct may be construed as illegal discrimination or harassment related to a protected class as set forth in Board policy AC (if so, the Principal shall confer with the District staff member(s) charged with handling such discrimination or harassment to determine how to proceed (e.g., parallel or combined investigations)); and

c. whether such conduct constitutes a safe schools violation requiring a report pursuant to RSA 193-D:4 and Ed 317.05.

2. Parental Notice of Bullying Report — RSA 193-F:4, II(h). Within 48 hours of receiving a report of bullying, the Principal will notify the parents of any student reported as a victim of bullying, as well as the parents of any student who has been reported as a perpetrator of bullying. Such notification may be made by telephone, writing or personal conference. The date, time, method, and location (if applicable) of such notification and communication shall be included in the investigative report. Notifications shall be consistent with the applicable provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA) relative to the student privacy rights of each student indicated in the report.

   The Principal may request of the Superintendent a waiver of the parental notification requirement, which may be granted only if the Superintendent deems such a waiver to be in the best interest of either the alleged victim or alleged perpetrator. If the waiver is granted, it shall be documented in writing.

3. Bullying Across School Districts — RSA 193-F:4, I(j). In cases of bullying and/or cyberbullying across multiple school districts, the Principal shall commence an investigation and contact the other involved school district(s) to collaborate investigation efforts. In cases of bullying and/or cyberbullying across multiple states, the Principal shall also inform the New Hampshire attorney general's office.

F. Investigative Procedures - RSA 193-F:4, II(j)

1. Upon receipt of a report of bullying, the Principal shall, within 5 school days, initiate an investigation into the alleged act. If the Principal is directly and personally involved with a complaint or is closely related to a party to the complaint, then the Superintendent shall direct another district employee to conduct the investigation.

2. The investigation should include documented interviews with the alleged victim, alleged perpetrator and any witnesses. All interviews shall be conducted privately, and shall be confidential to the extent permitted by law. Each individual will be interviewed separately and at no time will the alleged victim and perpetrator be interviewed together during the investigation.

3. The investigation should include review of any available surveillance recordings subject to the provisions of applicable Board policies.

4. If the alleged bullying was in whole or in part cyberbullying, the Principal may ask students and/or parents to provide the District with printed copies of the e-mails, text messages, website pages, or other similar electronic communications, consistent with Board policy JIH and RSA 189:70. RSA 189:70, II(d). The Principal may not, however, take any of the following actions:

i. Require or request a student or prospective student to disclose or to provide access to a personal social media account through the student's or prospective student's user name, password, or other means of authentication that provides access;
ii. Require or request a student or prospective student to access a personal social media account in the presence of any employee of the educational institution in a manner that enables the employee to observe the contents of the personal social media account;
iii. Compel a student or prospective student to add anyone to his or her list of contacts associated with a personal social media account or require, request, suggest, or cause a student or prospective student to change the privacy settings associated with a personal social media account;
iv. Take or threaten to take any action against a student or prospective student to discipline or prohibit such student or prospective student from participation in curricular or co-curricular activities for refusal to disclose information or to take the above actions.

RSA 189:70, I(a)-(d). The Principal may, however, monitor the usage of the District's computer network. In addition, the Principal may take any of the above listed actions if the social media account was created or provided by the District, if the student was provided advance notice that the account may be monitored at any time by District employees. RSA 189:70, III.

5. The Principal or other investigator shall consider all relevant facts and circumstances during the course of the investigation, including but not limited to:

   a. Description of incident, including the nature of the behavior;

   b. How often the conduct occurred;

   c. Whether there were past incidents or past continuing patterns of behavior;

   d. The characteristics of parties involved, (name, grade, age, etc.);

   e. The identity and number of individuals who participated in bullying behavior;

   f. Where the alleged incident(s) occurred;

   g. Whether the conduct adversely affected any student's education or educational environment;
   h. Whether the conduct physically harmed the alleged victim;
   i. Whether the conduct damaged the alleged victim's property;
   j. Whether the conducted caused emotional distress to a pupil;

   k. Whether the conduct was motivated by an imbalance of power based on the pupil's actual or perceived personal characteristics, behaviors, or beliefs, and/or motivated by the pupil's association with another person and based on the other person's characteristics, behaviors, or beliefs.;

   l. Whether the conduct violated any District or school policies or rules; and

m. The date, time and method by which parents or legal guardians of all parties involved were first contacted.

6. The Principal shall complete the investigation within 10 school days of receiving the initial report. If the Principal needs more than 10 school days to complete the investigation, the Superintendent may grant an extension of up to 7 school days. In the event such extension is granted, the Principal shall notify in writing all parties involved of the granting of the extension.

   Without limiting what might constitute sufficient cause for an extension under this paragraph, the Superintendent may consider the interests of the victim or alleged perpetrator related to any investigation into some or all of the same alleged conduct which other investigation includes procedures and timelines mandated by a regulation or statute other than RSA 193-F (e.g., Title IX, criminal investigations, etc.). Before waiving the time requirement on account of such other investigation, the Superintendent should confer with counsel and or the District's Title IX Officer.

G. Completion of Investigation and Report

1. Investigative Determination and Report: Whether a particular action or incident constitutes bullying/cyberbullying, retaliation or other violation of this policy – requires review and consideration of available evidence of all facts and surrounding circumstances. The investigative determination along with a summary of the investigation, shall be included in a comprehensive report. If the determination is that the bullying allegation is substantiated, the report shall include provisions describing any disciplinary consequences, interventions, supportive measures or other assistance for the victim or perpetrator, and, when indicated, any steps appropriate to protect all students from retaliation of any kind. The report may also include policy, training or other recommendations for preventing future bullying conduct within the school.

2. Communication with Students and Parents Upon Completion of Investigation - RSA 193-F:4, II(m).

   a. The Principal will meet promptly with each student (alleged victim and alleged perpetrator) involved in the incident(s) and communicate the general investigative determination as to whether the allegations of bullying/cyberbullying were substantiated, and any initial consequences or interventions appropriate to the determination.

   b. Within 10 school days of the completion of the investigation, the Principal will notify the parents of the alleged victim and of the alleged perpetrator of the outcome of the investigation and the school's remedies and assistance, within the boundaries of applicable state and federal law. The initial communication may be in writing, in person or by telephone, but if verbally, the Principal will also send a letter confirming earlier determination to the parents within 2 school days confirming the earlier notification.

   c. If the parents request, the Principal shall schedule a meeting with them to further explain the investigative determination.

d. In accordance with the Family Educational Rights and Privacy Act and other laws concerning student privacy, the District will not disclose educational records of students, including the discipline and remedial action assigned to those students and the parents of other students involved in a bullying incident.

3. Appeals: A parent aggrieved by the investigative determination of the Principal may appeal the determination in accordance with the standards and procedures set forth for Level II and Level III appeals in Board policy ACA.

4. Additional Reporting Requirements.

   a. Reporting Substantiated Incidents - RSA 193-F:4, II(l): The Principal shall forward all substantiated reports of bullying to the Superintendent upon completion of the Principal's investigation.

   b. Department of Education Reports - RSA 193-F:4, II(g): The Principal shall be responsible for completing such reports/forms as required by the New Hampshire Department of Education (NHED) for all substantiated incidents of bullying. Irrespective of the time/date a form/report is due to be filed with NHED, the report/form or the information required for the report/form shall be completed/compiled within 10 school days following an investigative finding of a substantiated bullying/cyberbullying report. The Principal or designee shall retain a copy and shall forward one copy to the Superintendent. Hard copies are not necessary if the digital form/data is retained and accessible to both the building administration and SAU.

   c. Reporting to NH Department of Education - RSA 193-F:6, I. The Superintendent shall annually report the District's substantiated incidents of bullying to the New Hampshire Department of Education. Pursuant to FERPA, such reports shall not contain any personally identifiable information pertaining to any student.

H. Substantiated Instances of Bullying/Cyberbullying, Retaliation or False Accusations: Interventions, Remedial Measures and Disciplinary Consequences — RSA 193-F:4, II(k).

While students who have been found to have committed an act of bullying/cyberbullying, or engaged in retaliation or made a false accusation, can face disciplinary consequences, the Board encourages the administration and school district staff to explore alternative or additional measures and interventions to address the substantiated instances of bullying/cyberbullying, and prevent their reoccurrence.

1. Interventions and Other Remedial Measures: Examples of interventions and remedial measures include, but are not limited to:

   a. Restitution,

   b. Parent conferences,

   c. Student counseling,

   d. Behavior assessment,

   e. Corrective instruction or other relevant learning experience,

f. Peer support group, and

g. Mediation (but only after the investigation has been completed).

Interventions and other remedial measures shall be designed to correct the problem behavior, prevent another occurrence of the problem, protect and provide support for the victim, and take corrective action for documented systematic problems related to bullying.

A finding that an allegation of bullying/cyberbullying, retaliation, or a false accusation is unsubstantiated *does not* preclude the District from implementing interventions and other remedial measures, when appropriate to do so.

2. Disciplinary Consequences - RSA 193-F:4, II(d)- Disciplinary consequences for students shall be consistent with District policies and the student handbook for the conduct that violated this policy. Disciplinary consequences should be varied according to specific circumstances such as: the nature of the behavior, the developmental age of the student, the student's prior disciplinary history, performance. Students will be afforded any due process applicable to the level of consequences as provided in Board policy JICD, RSA 193:13 and Ed 317.

I. Dissemination of Policy and Bullying Prevention Education - RSA 193-F:4, II(e) and 193-F:5.

1. Staff and Volunteers: All staff will be provided with a copy of this policy annually. The Superintendent may determine the method of providing the policy (employee handbook, hard copy, website, workshops, etc.). The Superintendent will ensure that all school employees and volunteers receive **annual** training on bullying and related Board policies, consistent with RSA 193-F:5.

2. Students: All students will be provided with a copy of this policy annually. The Superintendent may determine the method of providing the policy (student handbook, mailing, hard copy, website, etc.).

   Each year, all students will participate in programming that includes anti-bullying/cyberbullying materials presented in age-appropriate language. The materials and information should, among other things, describe expectations for student behavior, emphasize an understanding of what bullying/cyberbullying, harassment and intimidation is and looks like, the District's prohibition of such conduct and the reasons why the conduct is destructive, unacceptable, and how and when the conduct can lead to disciplinary consequences.

   The Superintendent, in consultation with staff, will, to the extent reasonably possible, integrate student anti-bullying training and education into the district's curriculum, behavior programs and other violence prevention efforts.

3. Parents: The Superintendent will ensure that all parents are annually provided with a copy of this policy or informed in writing where a copy of the policy may be located on the District and/or school's website. Student/family handbooks will include information of the District/school's anti-bullying program, as well as the means for students to report bullying acts either experienced or witnessed, and how parents, themselves, may inform/report to the school when they believe their child is being bullied or is bullying other students and encourage their

children to report bullying when it occurs.

4. Additional Notice and School District Programs: The Board may, from time to time, host or schedule public forums in which it will address this anti-bullying policy, discuss bullying in the schools, and consult with a variety of individuals, including teachers, administrators, guidance counselors, school psychologists and other interested persons.

J. Summary of School Officials' Duties to Implement Policy - RSA 193-F:4, II(n)

The Superintendent, as the person charged with supervision of all employees of the District, is responsible for the implementation of this policy and the provisions of RSA 193-F. The School Principal(s) are expected and required by statute to implement this policy within their respective school buildings and ensure the procedures are followed.

Consistent with this Policy, the Principal(s) shall receive reports of alleged bullying or retaliation, investigate the alleged conduct, and communicate with the parties involved (including their parents) consistent with privacy laws, and communicate/report to the Superintendent. The Superintendent shall oversee the Principal(s) in their duties relative to this policy and shall ensure each school is compliant with this policy. Additionally, the Superintendent, will receive reports of substantiated incidents, review waivers and time extension requests, and communicate with the Principal(s), the School Board, and the NH Department of Education, all as provided in this policy.

K. Immunity and Liability – RSA 193-F:7 & 9

Under 193-F:7, employees, volunteers, students, parents and any other person covered by this policy will be immune from civil liability for **good faith** conduct arising from or pertaining to the reporting, investigation, findings, recommended response, or implementation of a recommended response under this policy or RSA 193-F. (Note – civil liability could arise, (including for attorney fees) in the event of gross negligence or willful misconduct for violations of this policy.)

Legal References:

RSA 193-F, Pupil Safety and Violence Prevention Act

RSA 187:70, Educational Institution Policies on Social Media

RSA 570-A:2, Capture of Audio Recordings on School Buses Allowed

NH Code of Administrative Rules, Section Ed 306.04(b)(7), Student Harassment

1st Reading: October 26, 2010
2nd Reading: November 23, 2010
3rd Reading: November 23, 2010 (Waived)
Adopted: November 23, 2010

1st Reading: June 22, 2022
2nd Reading: September 28, 2022
3rd Reading: November 2, 2022 (as amended)
Adopted: November 2, 2022

1st reading: August 23, 2023 (as amended)
2nd Reading: September 27, 2023
3rd & Adopt: November 29, 2023

~~1st Reading: September 15, 2010~~
~~2nd Reading: November 17, 2010~~
~~Adopted: November 17, 2010~~

~~1st Reading: December 11, 2019~~
~~2nd Reading: January 22, 2020~~
~~Adopted: February 12, 2020~~

1st Reading: December 17, 2025
2nd Reading: April 22, 2026 (as amended)
3rd Reading: June 10, 2026~~)~~

Policy EBCA: Crisis Prevention and Emergency Response Plans

Category: Recommended
References: JICI, EBCH, JLCJA, EB, EBB, EBCB, EBCD, JICK, EBCC

The Board recognizes that schools are subject to a number of potentially dangerous events, such as natural disasters, industrial accidents, acts of terrorism, and other violent events. No school is immune from these events no matter the size or location. The Board is committed to the prevention of these events, to the extent possible, in the schools and at school-sponsored activities.

District-Wide Plans

The Superintendent, in coordination with school administrators and local emergency authorities, shall maintain a comprehensive District Emergency Operations Plan ("EOP") in accordance with RSA 189:64, the Incident Command System (ICS), and the National Incident Management System (NIMS).

The District EOP shall serve as both the site-specific emergency operations plan for each school and the District-wide Crisis Prevention and Response Plan. The plan shall address, but not be limited to, acts of violence, threats, natural disasters, fire, hazardous materials, medical emergencies, sports injury emergency response, and other hazards deemed necessary by the School Board or local emergency authorities.

The Superintendent or designee shall annually review and update the District EOP in coordination with building administrators and emergency response agencies. If, after such review, the plan remains unchanged, the Superintendent/Principal shall notify the New Hampshire Department of Safety by October 15 that the plan is unchanged. If the Emergency Operations Plan is updated or revised, the Superintendent/Principal shall submit the updated plan to the Director of Homeland Security and Emergency Management of the Department of Safety by October 15.

The District Emergency Operations Plan shall not be considered a public record and shall not be available for public inspection or review, except as otherwise required by law.

All emergency response drills, including fire and all-hazard drills, shall be conducted annually in accordance with Board policy and applicable state law.

School building principals, or their designee, shall annually review their site-specific EOP and submit updated plans (or report of no changes) to the Superintendent for review by October 1st. Members of the public will not be permitted to view the EOP.

If, after such review, the plan remains unchanged, then the Principal shall notify the New Hampshire Department of Safety by October 15 that the plan is unchanged. If an Emergency Operations Plan is updated/revised, the Principal shall submit the updated Emergency Operations Plan to the Director of Homeland Security and Emergency Management of the Department of Safety by October 15.

Coordination

The Superintendent will establish a relationship with local and state emergency services (e.g., police, fire, ambulance, etc.). Unless otherwise provided in a site-specific EOP, the District

Crisis Prevention and Response Plan or the District Communication Plan, the Superintendent, or their designee, will serve as the coordinator/liaison with these authorities. Additionally, the Superintendent should designate personnel to explore the availability of any training or support provided by the New Hampshire Departments of Education and/or Safety associated with risk assessment, crisis management, and other matters related to this policy.

NH Statutes	**Description**
RSA 153-A:28-33	Automated External Defibrillation
RSA 189:64	Emergency Response Plans
RSA 193-D	Safe School Zones
RSA 193-F	Pupil Safety and Violence Prevention
RSA 200:40-c	Emergency Plans for Sports Related Injuries

NH Dept of Ed Regulation	**Description**
N.H. Code Admin. Rules Ed 306.04(b)(2)	School Safety

1st Reading: May 27, 2026

2nd Reading: June 10, 2026

Policy: IMG

Section: Section I - Instruction

(BSD) Animals in the Classroom

IMG

Category O

ANIMALS IN THE CLASSROOM

It is the policy of the Brookline School Board that animals shall not be permitted on school grounds ~~at any time~~ during school hours or during school-sanctioned events unless permission has been granted by the building principal. However, the Board recognizes that under the proper conditions, animals can be an effective teaching aid. In order to protect both children and animals, the superintendent or designee shall establish guidelines for authorized animals to be on school grounds that address the following issues:

1. The bringing of animals into the classroom must not violate city/state/federal ordinances.
2. Animals allowed in a classroom must be for a specific and appropriate educational purpose.
3. All animals must be in good physical condition and vaccinated against transmittable diseases.
4. Special consideration should be given to the effect of animals on allergic children.
5. The animal will be kept in an appropriate cage or container and fecal material will be handled in a sanitary manner.
6. Service dogs are considered authorized animals per Policy IMGA.

Unauthorized animals are not allowed in school buildings or on school grounds during school hours and during school-sanctioned events. Children and staff will be instructed to keep their own animals off the school grounds. The appropriate town official will be called and requested to impound all animals taken into custody by school personnel.

1st Reading: May 22, 2012
2nd Reading: June 26, 2012
3rd Reading: July 24, 2012
Adoption: July 24, 2012

1st Reading: June 12, 2019 (as amended)
2nd Reading: October 23, 2019
3rd Reading: November 20, 2019
Adopted: November 20, 2019

1st Reading: May 27, 2026 (as amended)
2nd Reading: June 10, 2026

BEDB: Agenda Preparation and Dissemination

Category: Recommended

The purpose of this policy is to establish a clear and consistent process for preparing School Board meeting agendas in accordance with RSA-91-A and the principles of governance.

The Superintendent shall prepare all agendas for ~~meetings of the~~ Board *meetings*. In doing so, the Superintendent (or designee) shall ~~consult and~~ *collaborate* with the Board Chair *in its development and finalization prior to public posting*. *A requested item shall be included on the agenda unless either the Superintendent or the Board Chair determines that an item is not appropriate for placement or restriction due to legal policy or procedural reasons. Any item that has a legal, policy, or procedural reason for its placement or removal on an agenda will be included.*

Items to be placed on the agenda should be received by the Superintendent at least ten days prior to the meeting. *Any Board member, staff member, student, or citizen of the District may suggest items of business.* ~~*The inclusion of items suggested by staff members, students, or citizens shall be at the discretion of the Board Chairperson.*~~ ~~Every Board member has the right to place items on the agenda.~~ *Requests for items to be included on an agenda shall be submitted as follows:*

- *SAU administrators, staff, and students shall submit requests to the Superintendent.*
- *School Board members shall submit requests to the Board Chair.*
- *Parents, guardians, or citizens may submit requests for agenda items to either the Superintendent or the Board Chair.*

Matters not included in the agenda may be presented during the meeting, provided the Board agrees to discuss the matter *and the Superintendent is consulted on the legality and appropriateness of public discussion*. The Board may choose not to deal with every agenda item.

Consistent with RSA 91-A:3 and the laws pertaining to student and family privacy rights, the Board will not place any matter on the public meeting agenda that is to be properly discussed in a non-public session. This shall not preclude the Board from giving notice of its intent to hold or enter into a non-public session and the statutory reason for doing so.

~~Any Board member, staff member, student, or citizen of the District may suggest items of business. The inclusion of items suggested by staff members, students, or citizens shall be at the discretion of the Board Chairperson. The Board Chair shall work in collaboration with the Superintendent in the development and finalization of the agenda.~~

The Board shall follow the order of business set up by the agenda unless the order is altered by a majority vote of the members present. Items of business not on the agenda may be discussed and acted upon if a majority of the Board agrees to consider them. The Board, however, may not revise Board policies~~,~~ or adopt new ones~~,~~ unless such action has been scheduled or unless there is an emergency.

The agenda and supporting materials should be posted online at least three days prior to the Board meeting. Board Members shall be expected to read the information provided *to* them and to contact the Superintendent to request additional information ~~that may be~~ deemed necessary to assist them in their decision-making responsibilities.

~~When~~ *Once* the final agenda ~~has been~~ *is* established, it will be made available to the public online. Members of the public who wish to speak at Board meetings regarding an agenda item are encouraged to contact the Superintendent prior to the Board meeting. Additionally, the Board reserves the right to limit public discussion at Board meetings to agenda items only.

A consent agenda may be used at School Board meetings to cover the following actions: accepting resignations and/or nominations for professional staff persons when supported by written documentation.

NH Statutes	**Description**
RSA 91-A:3	Non-Public Sessions
RSA 91-A:5	Exemptions (Access to Governmental Records)

Cross References

Code	**Description**
BEDA	Public Notification of School Board Meetings
BEDDA	Board Meeting - Rules of Procedure & Order
BEDH	Public Comment and Participation at Board Meetings

1st Reading: November 26, 2013 (Amended)
2nd Reading: December 10, 2013
3rd Reading: January 28, 2014
Adopted: January 28, 2014

1st Reading: March 25, 2026 (as amended)

2nd Reading: April 22, 2026
3rd Reading: Waived
Adopted: April 22, 2026

1st Reading: May 27, 2026 (as amended)
2nd Reading: June 10, 2026