

Hollis Brookline Cooperative School District

Expendable Trust: Public Hearing

June 19, 2019

Maintenance Expendable Trust

Background

The elevator at HBMS is approximately 30 years old. While it is still safe and in working order it does need more and more repairs to keep it going. The problem is not making the repairs but finding the parts. This past fall the elevator stopped working due to an inoperable traveling cable. After an extensive search another traveling cable that would fit was found. The repair was made buying HBMS another 3-5 years.

FY19 Request for Repair Cost

HBMS Replace Traveling Cable \$10,030 (end of life)

Maintenance Expendable Trust

Current Balance: \$ 122,205
FY19 Expenditures: \$ 10,030
To be added in FY20: \$ 75,000
FY20 Expenditures: \$ 95,000 per FY20 Budget Documents
Resulting Balance: \$ 92,175 Fall of 2019

Athletic Expendable Trust

Background

The Athletic Expendable Trust is funded by parent paid athletic fees. The total fees collected in one year are sent to the Trust in the following year. An annual request and public hearing occurs each year to spend all or part of that allocation. This year's request is for athletic expenses that were assigned to the Athletic Trust Account via the budget process and are as follows:

FY19 Request for Purchases

	FY19 Budget for Athletic Trust	Actual	
Description	Reimbursement	Costs	Balance
Field Maintenance	\$8,750.00	\$6,950.00	\$1,800.00
Equipment Repair	\$2,599.00	\$0.00	\$2,599.00
Transportation	\$3,668.68	\$3,668.68	\$0.00
Transportation	\$12,831.32	\$12,171.02	\$660.30
Training Supplies	\$3,044.02	\$3,626.60	(\$582.58)
Athletic Supplies	\$242.90	\$237.48	\$5.42
Awards	\$3,000.00	\$1,538.88	\$1,461.12
Uniforms	\$202.00	\$202.00	\$0.00
Uniforms	\$10,083.08	\$10,083.08	\$0.00
Addl Equipment	\$3,000.00	\$2,452.00	\$548.00
Addl Equipment	\$8,199.00	\$7,883.00	\$316.00
Replacement Equipment	\$5,602.00	\$5,406.00	\$196.00
Dues and Fees	\$5,778.00	\$5,778.00	\$0.00
Total	\$67,000.00	\$59,996.74	\$7,003.26

Athletic Expendable Trust

Current Balance: \$ 101,065
FY19 Expenditures: \$ 59,997
To be added in FY20: \$ 67,000
FY20 Expenditures: \$ 67,000 per FY20 Budget Documents
Resulting Balance: \$ 41,068 6/30/20

To: Hollis Brookline Cooperative School Board
From: Bob Thompson, Principal HBMS
Re: Principal's Report
Date: June 19, 2019, Scheduled Meeting

INFORMATION ONLY

Teacher of the Year: Congratulations to HBMS Health Teacher Erin White who was the recipient of the 2019 Hillsborough County Conservation Commission Teacher of the Year. Erin was awarded this honor as a result of her continuing efforts with our community greenhouse. Erin was honored in a ceremony held at the Lawrence Barn on May 31st.

Emergency Preparedness Conference: On June 4th HBMS staff presented at the Annual Emergency Management Conference hosted by the Department of Homeland Security. Presenters included: Lynn DiZazzo, Katie Williamson, Bob Thompson and Rick Bergeron. The presentation entitled, Teachers are First Responders Too; one school's journey to create a culture of safety and emergency preparedness for all, was well attended and received a great deal of positive feedback. HBMS has been asked to return for next year's conference.

Governor for the Day: 8th grade student, Chris Pyle, was selected as the winner of the 2019 'Governor for a Day' competition. Chris joined Governor Christopher T. Sununu at the State House in Concord on Monday, June 3, 2019, for a day full of educational experiences. Chris served as the official student 'Governor for a Day' and was publicly recognized as such. His essay was chosen based on the innovative, forward-thinking approach it displayed.

The 'Governor for a Day' initiative was launched in New Hampshire to foster civic education and promote youth participation in government. The competition was open to all middle and high school students across the Granite State. Applicants submitted a 250-500 word essay completing the sentence, "If I were Governor for a day, I would..."

Team Assignments: All of our incoming 7th and 8th grade students have been placed on their teaching teams for next year. I want to thank Patti Flynn who invested a tremendous amount of time ensuring that teams were heterogeneously mixed. The process is time-intensive and involves reviewing parent feedback, analyzing standardized testing data, and reviewing teacher recommendations.

6th Grade Step Up Day: On June 11th, 6th graders from CSDA and HUES had the opportunity to attend step up day at HBMS. The day includes an opportunity for students to meet their team of teachers for next year, tour the building, and participate in some team building activities.

8th Grade Step Up: On June 18th, 8th graders will walk to Hollis Brookline High School for step up day. The program will begin at 12:45 in the HBHS Auditorium. Students will also receive copies of their schedules for next year.

Student Recognition Assembly: Our student recognition assembly is scheduled for June 19th at 7:45 am in the HBMS gymnasium. This is an opportunity for us to recognize the hard work and commitment that our students have demonstrated throughout the year. The day will culminate with the 7th grade barbecue and the 8th graders traveling to Canobie Lake Park.

Registration Day: On August 21st and 22nd HBMS will host its annual registration. Registration day is an opportunity for students to come to school prior to the start of the school year. Students receive their schedule, locker number and are able to tour the building.

From: Rick Barnes, Principal
To: Andrew Corey, Superintendent
RE: June Board Report

Graduation: Family and friends of the Class of 2019 could not have asked for better weather for the ceremony last weekend. It was estimated that 2,000 people attended the event. Thanks to the efforts of the Graduation Committee as led by Kristine Bumpus, custodians, and staff the day ran incredibly smooth.

2019 Seatbelt Challenge State Champs! Congratulations to Maddi Norris, Maddi Richardson, Mike Moscatelli, and Victoria Harris as led by Officer Bergeron for their victory in Concord!

Retail Therapy: Thank you to everyone who supported the Retail Therapy Fashion show during the month of May. Mrs. Candice Hancock orchestrated this successful event that served to create awareness for mental health as well as raising over \$500 in donations for Bridges in Nashua.

Technology Plan: We look forward to presenting phase one of the HBHS Five Year Technology Plan at the July Board Meeting

PSAT: Beginning October 2019, we will be expanding access to the PSAT to all sophomores who wish to pay and take the exam. Families will be notified on how to sign up for the exam this month so we will have the appropriate number needed in the fall.

Respectfully Submitted,

Rick Barnes
Principal

Participation Numbers: Overall participation numbers for the Spring season are up across the district, with the addition of Boys and Girls Lacrosse at HBMS.

SCHOOL	SPORT	17-18	18-19
HS	Baseball	32	27
HS	Boys Lacrosse	38	32
HS	Boys Tennis	9	13
HS	Boys Volleyball	29	32
HS	Girls Lacrosse	37	40
HS	Girls Tennis	11	13
HS	Outdoor Track	53	51
HS	Softball	28	28
HS	Unified Track	31	21
MS	Baseball	18	17
MS	Boys Lacrosse	N/A	21
MS	Girls Lacrosse	N/A	21
MS	Outdoor Track	72	60
MS	Softball	15	15
TOTAL		373	391

Recent Coaching Hires:

Bass Fishing Head Coach (HBHS) – Jack Cadario

Bass Fishing Asst. Coach (HBHS) – Tammy Salisbury

Golf Head Coach (HBHS) – Shaun Hastings

District Coaching Openings: The HB Athletic Department is currently looking for qualified candidates to fill the following coaching vacancies.

Field Hockey JV Coach (HBHS)

Cross Country Head Coach (HBHS)

Cross Country Asst. Coach (HBHS)

Golf Asst. Coach (HBHS)

Boys Reserve Soccer Head Coach (HBHS)

Skiing Head Coach (HBHS)

Skiing Asst. Coach (HBHS)

Boys Lacrosse Asst. Coach (HBHS)

Girls Tennis Head Coach (HBHS)

Respectfully Submitted,



Brian Bumpus
District Athletic Coordinator

Hollis Brookline Cooperative School District

FY19 YTD Expense and Revenue Report

As of 6/11/2019

Expenses				
Description	Budget	YTD Expense	Encumbered	Balance
Regular Education	\$ 5,701,951	\$ 4,661,862	\$ 1,007,422	\$ 32,667
Special Education	\$ 3,520,464	\$ 2,938,578	\$ 461,843	\$ 120,042
Vocational Program	\$ 40,840	\$ 16,305	\$ 17,808	\$ 6,727
Co-curricular Program	\$ 748,177	\$ 688,557	\$ 51,098	\$ 8,522
Student Support Services	\$ 1,352,346	\$ 1,029,701	\$ 265,304	\$ 57,341
Instructional Staff Support	\$ 703,406	\$ 476,987	\$ 125,796	\$ 100,623
*School Board/SAU Assessment	\$ 977,608	\$ 854,714	\$ 12,163	\$ 110,731
School Administration	\$ 1,076,405	\$ 973,639	\$ 88,413	\$ 14,353
Facilities	\$ 1,274,582	\$ 1,118,615	\$ 104,736	\$ 51,232
Transportation	\$ 1,120,522	\$ 994,766	\$ 204,052	\$ (78,297)
Benefits	\$ 4,740,915	\$ 3,973,357	\$ 743,691	\$ 23,868
Site improvements	\$ 75,500	\$ 70,418	\$ -	\$ 5,082
Debt Service	\$ 620,191	\$ 595,867	\$ -	\$ 24,324
Transfers	\$ 2,474,000	\$ 1,816,133	\$ 654,000	\$ 3,868
TOTAL	\$ 24,426,907	\$ 20,209,498	\$ 3,736,327	\$ 481,082

FY18 Expense Carryover	\$152,203	\$119,401	\$5,220	\$27,582
TOTAL FY18 + FY19	\$ 24,579,110	\$ 20,328,899	\$ 3,741,547	\$ 508,664

* Please note that the \$100,000 Contingency fund is not encumbered; no planned use at this time.

Revenue

Description	Budget	YTD Revenue	Expected	Balance
Local Property Tax	\$ 17,436,813	\$ 16,736,813	\$ 700,000	\$ -
Adequacy Aid Grant/Tax	\$ 3,016,549	\$ 3,016,549		\$ -
Impact Fees	\$ 5,000	\$ 20,374		\$ 15,374
State				\$ -
Special Education Aid	\$ 594,000	\$ 586,177	\$ -	\$ (7,823)
Building Aid	\$ 181,362	\$ 181,362		\$ -
Food Service	\$ 3,000	\$ 3,334		\$ 334
Federal				\$ -
Grants	\$ 260,000	\$ 60,416	\$ 199,584	\$ -
Food Service	\$ 38,000	\$ 35,663	\$ 2,337	\$ -
Medicaid	\$ 146,457	\$ 73,072	\$ 23,000	\$ (50,385)
Local				\$ -
Tuition	\$ 5,000	\$ 7,353		\$ 2,353
Food Service Sales	\$ 353,000	\$ 355,003		\$ 2,003
Other	\$ 5,000	\$ 96,260		\$ 91,260
Contingency & Trusts	\$ 260,000	\$ 260,000		\$ -
Capital Projects	\$ 1,660,000	\$ 1,660,000		\$ -
Unreserved Fund Balance	\$ 604,726		\$ 604,726	\$ -
Less Retained Fund Balance	\$ (142,000)		\$ (142,000)	\$ -
TOTAL REVENUE	\$ 24,426,907	\$ 23,092,376	\$ 1,387,647	\$ 53,116

Total Expense Balance	\$508,664
Total Revenue Balance	\$53,116
Unreserved Fund Balance	\$561,780

Anticipated Reductions to Unreserved Fund Balance

Contingency	\$ 100,000
Athletic Trust	\$ 67,000
Maint. Trust	\$ 75,000
Spec Ed Trust	\$ 25,000
Retained Fund Balance	\$ 142,000
Total Reductions	\$ 409,000

Projected Unreserved Fund Balance [Returned to Taxpayers] \$152,780

Explanation of budget balances on current expense report

6/11/2019

Function	Description	Current Balance	Notes
1100	Regular Education	\$ 32,667	Staffing changes; fewer lane changes than expected
1200	Special Education	\$ 120,042	Savings in salaries, OOD tuition, tutoring, and services
1300	Vocational Program	\$ 6,727	Lower # of voc ed students than budgeted
1400	Co-curricular Program	\$ 8,522	Some athletic assistant stipends not filled; lower academic competition fees
2100	Student Support Services	\$ 57,341	Savings in consultations
2200	Instructional Staff Support	\$ 100,623	Savings in teacher professional development and MLP reimbursements
2300	School Board/SAU Assessment	\$ 110,731	\$100K contingency fund not being used; lower legal expenses
2400	School Administration	\$ 14,353	Savings in service agreements and replacement equipment
2600	Facilities	\$ 51,232	Savings in custodial salaries due to unfilled positions and in snow removal
2700	Transportation	\$ (78,297)	Vocational Education transportation - lease of vans postponed
2900	Benefits	\$ 23,868	Savings in teacher NH retirement (lower rate)
4000	Site improvement	\$ 5,082	
5100	Debt Service	\$ 24,324	Turf field bond interest postponed to FY20's budget
5200	Transfers	\$ 3,868	Athletic Trust transfer \$66,132 instead of \$70,000
	TOTAL	\$ 481,082	

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
1300	Vocational Program	Vocational ed. Tuition
1400	Co-curricular Program	Athletic program and other co-curricular activities
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	Debt Service	Principal and interest payments on bonds
5200	Transfers	Accounting line to make total expenses match total revenue, and match the budget.

FY20 ATHLETIC STIPENDS - HBHS

SEASON	SPORT	POSITION	TOTAL
Spring	Baseball	JV	\$2,600.00
Spring	Baseball	Asst.	\$1,900.00
Spring	Baseball	Head	\$3,750.00
Winter	Basketball - Boys	Head	\$4,700.00
Winter	Basketball - Boys	FR	\$1,900.00
Winter	Basketball - Boys	JV	\$2,950.00
Winter	Basketball - Girls	JV	\$2,950.00
Winter	Basketball - Girls	Head	\$4,700.00
Winter	Basketball - Unified	Head	\$1,900.00
Winter	Basketball - Unified	Asst.	\$1,200.00
Fall	Bass Fishing	Head	\$1,900.00
Fall	Bass Fishing	Asst.	\$900.00
Winter	Bowling	Asst.	\$1,900.00
Winter	Bowling	Head	\$2,600.00
Fall	Cross Country	Head	\$4,125.00
Fall	Cross Country	Asst.	\$1,900.00
Fall	Cross Country	Asst.	\$1,900.00
Winter	Faculty Manager	Head	\$2,600.00
Fall	Field Hockey	Head	\$4,125.00
Fall	Field Hockey	Asst.	\$1,900.00
Fall	Field Hockey	JV	\$2,950.00
Fall	Football	Asst.	\$2,600.00
Fall	Football	Head	\$4,700.00
Fall	Football	JV	\$3,750.00
Fall	Football	Asst.	\$2,600.00
Fall	Football	Asst.	\$2,600.00
Fall	Golf	Head	\$2,950.00
Fall	Golf	Asst.	\$1,200.00
Winter	Gymnastics	Head	\$1,900.00
Winter	Ice Hockey	Head	\$4,125.00
Spring	Lacrosse - Boys	JV	\$2,600.00
Spring	Lacrosse - Boys	Head	\$3,750.00
Spring	Lacrosse - Boys	Asst.	\$1,900.00
Spring	Lacrosse - Girls	Asst.	\$1,900.00
Spring	Lacrosse - Girls	Head	\$3,750.00
Spring	Lacrosse - Girls	JV	\$2,600.00
Winter	Ski Team	Head	\$2,950.00
Winter	Ski Team	Asst.	\$1,900.00
Winter	Ski Team	Bus	\$900.00
Fall	Soccer - Boys	JV	\$2,950.00
Fall	Soccer - Boys	Head	\$4,125.00
Fall	Soccer - Boys	Asst.	\$1,900.00
Fall	Soccer - Girls	Head	\$4,125.00
Fall	Soccer - Girls	Asst.	\$1,900.00

HBHS

Fall	Soccer - Girls	JV	\$2,950.00
Fall	Soccer - Unified	Head	\$1,900.00
Fall	Soccer - Unified	Asst.	\$1,200.00
Spring	Softball	Asst.	\$1,900.00
Spring	Softball	JV	\$2,600.00
Spring	Softball	Head	\$3,750.00
Fall	Spirit - Fall	Head	\$2,600.00
Fall	Spirit - Fall	Asst.	\$1,900.00
Winter	Spirit - Winter	Head	\$3,750.00
Winter	Spirit - Winter	Asst.	\$1,900.00
Winter	Swimming	Asst.	\$1,900.00
Winter	Swimming	Head	\$2,950.00
Spring	Tennis - Boys	Head	\$2,950.00
Spring	Tennis - Boys	Asst.	\$1,200.00
Spring	Tennis - Girls	Head	\$2,950.00
Spring	Tennis - Girls	Asst.	\$1,200.00
Winter	Track - Indoor	Asst.	\$2,600.00
Winter	Track - Indoor	Head	\$3,750.00
Spring	Track - Outdoor	Assoc.	\$2,950.00
Spring	Track - Outdoor Boys	Head	\$3,750.00
Spring	Track - Outdoor Boys	Asst.	\$1,900.00
Spring	Track - Outdoor Girls	Asst.	\$1,900.00
Spring	Track - Outdoor Girls	Head	\$3,750.00
Spring	Track - Unified	Head	\$1,900.00
Spring	Track - Unified	Asst.	\$1,200.00
Spring	Volleyball - Boys	JV	\$2,600.00
Spring	Volleyball - Boys	Head	\$3,750.00
Fall	Volleyball - Girls	Head	\$4,125.00
Fall	Volleyball - Girls	FR	\$1,900.00
Fall	Volleyball - Girls	JV	\$2,950.00
Winter	Wrestling	Head	\$4,700.00
Winter	Wrestling	Asst.	\$1,900.00
TOTAL			\$202,250.00

FY20 ATHLETIC STIPENDS - HBMS

SEASON	SPORT	POSITION	TOTAL
Spring	Athletic Director	Head	\$3,000.00
Fall	Athletic Director	Head	\$3,000.00
Spring	Baseball	Head	\$2,500.00
Winter	Basketball - Boys	Head	\$2,900.00
Winter	Basketball - Girls	Head	\$2,900.00
Fall	Cross Country	Head	\$2,500.00
Fall	Cross Country	Head	\$2,500.00
Fall	Field Hockey (1 of 2)	Head	\$1,250.00
Fall	Field Hockey (2 of 2)	Head	\$1,250.00
Spring	Lacrosse - Boys	Head	\$2,500.00
Spring	Lacrosse - Girls	Head	\$2,500.00
All	Play-offs	All	\$2,500.00
Fall	Soccer - Boys (1 of 2)	Head	\$1,250.00
Fall	Soccer - Boys (2 of 2)	Head	\$1,250.00
Fall	Soccer - Girls	Head	\$2,500.00
Fall	Softball	Head	\$2,500.00
Spring	Track - Outdoor	Head	\$2,500.00
Spring	Track - Outdoor	Head	\$2,500.00
Spring	Track - Outdoor	Head	\$2,500.00
Spring	Track Stats	Head	\$500.00
Fall	Volleyball	Head	\$2,500.00
Winter	Wrestling	Head	\$2,900.00
TOTAL			\$50,200.00

HOLLIS BROOKLINE MIDDLE SCHOOL - STIPEND TABLE 2019-2020

TIER 1 \$500	TIER 2 \$2,500	TIER 3 \$2,900	TIER 4 \$3,000
Track Stats	Baseball Cross Country 1 of 2 Cross Country 2 of 2 Field Hockey Lax - Boys Lax - Girls Play-offs TOTAL Soccer - Boys Soccer - Girls Softball - Girls Track and Field 1 of 3 Track and Field 2 of 3 Track and Field 3 of 3 Volleyball	Basketball - Boys Basketball - Girls Wrestling	Athletic Director Fall Athletic Director Spring

HOLLIS BROOKLINE HIGH SCHOOL - STIPEND TABLE 2019-2020

TIER 1 \$900	TIER 2 \$1,200	TIER 3 \$1,900	TIER 4 \$2,600
Bass Fishing Asst. Ski Team Bus Chaperone	Golf Asst. Tennis- Boys Asst. Tennis- Girls Asst. Unified Basketball - Asst. Unified Soccer - Asst. Unified Track - Asst.	Baseball - Asst. Basketball - Boys FR Bass Fishing Head Bowling - Asst. Cross Country - Asst. 1 of 2 Cross Country - Asst. 2 of 2 Field Hockey Asst. Gymnastics - Head Lacrosse - Boys Asst. Lacrosse - Girls Asst. Ski Team - Asst. Soccer - Boys Assistant Soccer- Girls Asst. Softball- Assistant Spirit- Fall - Asst. Spirit- Winter- Asst. Swimming Asst. Track - Spring Boys Asst. Track - Spring Girls Asst. Unified Basketball - Head Unified Soccer - Head Unified Track - Head Volleyball - Girls FR Wrestling - Asst.	Baseball - JV Bowling - Head Faculty Manager Football - Asst. 1 of 3 Football - Asst. 2 of 3 Football - Asst. 3 of 3 Lacrosse - Boys JV Lacrosse - Girls JV Softball - JV Spirit, Fall - Head Track - Indoor Asst. Volleyball - Boys JV
TIER 5 \$2,950	TIER 6 \$3,750	TIER 7 \$4,125	TIER 8 \$4,700
Basketball - Boys JV Basketball - Girls JV Field Hockey - JV Golf - Head Ski Team - Head Soccer - Boys JV Soccer - Girls JV Swimming - Head Tennis - Boys Head Tennis - Girls Head Track - Spring Associate Volleyball - Girls JV	Baseball - V Football - JV Lacrosse - Boys V Lacrosse - Girls V Softball - Varsity Spirit, Winter - Head Track - Indoor Head Track - Spring Boys Head Track - Spring Girls Head Volleyball - Boys V	Cross Country - Head Field Hockey - V Ice Hockey - Head Soccer - Boys V Soccer - Girls V Volleyball - Girls V	Basketball - Boys V Basketball - Girls V Football - V Wrestling - Head

Team Times and Core Rotation 2018-2019

Team #1-Summit

Period 1-	7:35	–	7:55	ROCK
Period 2-	7:58	–	9:09	Core
Period 3-	9:12	–	9:54	FL/Rdg/PE/Music/Skills
Period 4-	9:57	–	10:39	FL/Rdg/PE/Music/Skills (CPT)
Period 5-	10:42	–	11:53	Core
Period 6-	11:56	–	12:38	FL/Rdg/PE/Music/Skills
Period 7-	12:38	–	1:06	Lunch
Period 8-	1:09	–	2:20	Core

Rotation – Team #1					
	<u>Mon</u>	<u>Tues</u>	<u>Weds</u>	<u>Thurs</u>	<u>Fri</u>
Per 2	A	D	B	E	C
Per 5	B	E	C	A	D
Per 8	C	A	D	B	E

Team #2-Titan

Period 1-	7:35	–	7:55	ROCK
Period 2-	7:58	–	8:40	FL/Rdg/PE/Music/Skills (CPT)
Period 3-	8:43	–	9:54	Core
Period 4-	9:57	–	11:08	Core
Period 5-	11:11	–	11:53	FL/Rdg/Music/Skills
Period 6-	11:56	–	12:38	FL/Rdg/PE/Music/Skills
Period 7-	12:38	–	1:06	Lunch
Period 8-	1:09	–	2:20	Core

Rotation – Team #2					
	<u>Mon</u>	<u>Tues</u>	<u>Weds</u>	<u>Thurs</u>	<u>Fri</u>
Per 3	A	D	B	E	C
Per 4	B	E	C	A	D
Per 8	C	A	D	B	E

Team #3-da Vinci

Period 1-	7:35	–	7:55	ROCK
Period 2-	7:58	–	9:09	Core
Period 3-	9:12	–	9:54	FL/Rdg/PE/Music/Skills (CPT)
Period 4-	9:57	–	10:39	FL/Rdg/PE/Music/Skills
Period 5-	10:42	–	11:53	Core
Period 6-	11:53	–	12:21	Lunch
Period 7-	12:24	–	1:35	Core
Period 8 -	1:38	–	2:20	FL/Rdg/PE/Music/Skills

Rotation – Team #3					
	<u>Mon</u>	<u>Tues</u>	<u>Weds</u>	<u>Thurs</u>	<u>Fri</u>
Per 2	A	D	B	E	C
Per 5	B	E	C	A	D
Per 7	C	A	D	B	E

Team #4-Bartlett

Period 1-	7:35	–	7:55	ROCK
Period 2-	7:58	–	8:40	FL/Rdg/PE/Music/Skills
Period 3-	8:43	–	9:54	Core
Period 4-	9:57	–	11:08	Core
Period 5-	11:11	–	11:53	FL/Rdg/PE/Music/Skills (CPT)
Period 6-	11:53	–	12:21	Lunch
Period 7-	12:24	–	1:35	Core
Period 8-	1:38	–	2:20	FL/Rdg/PE/Music/Skills

Rotation – Team #4					
	<u>Mon</u>	<u>Tues</u>	<u>Weds</u>	<u>Thurs</u>	<u>Fri</u>
Per 3	A	D	B	E	C
Per 4	B	E	C	A	D
Per 7	C	A	D	B	E



HBMS DRAFT Bell Schedule 2019 – 2020

Monday	Tuesday (Odds)	Wednesday (Evens)	Thursday	Friday (PLCs)
Period 1 7:35 – 8:17 42 min.	Period 1 7:35 – 9:01 86 min.	Period 2 7:35 – 9:01 86 min.	Period 1 7:35 – 8:17 42 min.	Period 1 8:00 – 8:39 39 min.
Period 2 8:20 – 9:02 42 min.			Period 2 8:20 – 9:02 42 min.	Period 2 08:41 – 9:20 39 min.
Period 3 9:05 – 9:47 42 min.	Period 3 9:04 – 10:30 86 min.	Period 4 9:04 – 10:30 86 min.	Period 3 9:05 – 9:47 42 min.	Period 3 9:23 – 10:02 39 min.
Period 4 9:50 – 10:32 42 min.			Period 4 9:50 – 10:32 42 min.	Period 4 10:04 – 10:43 39 min.
Period 5 10:34 – 11:16 42 min.	Period 5 10:33 – 11:59 86 min.	Period 6 10:33 – 11:59 86 min.	Period 5 10:34 – 11:16 42 min.	Period 5 10:46 – 11:25 39 min.
Lunch & Rock 11:16 – 12:08 52 min.			Lunch & Rock 11:16 – 12:08 52 min.	Lunch & Rock 11:25 – 12:17 52 min.
Gr 8 Lunch/Gr 7 ROCK 11:16 – 11:42 26 min.	Lunch & Rock 12:00 – 12:52 52 min.	Lunch & Rock 12:00 – 12:52 52 min.	Gr 8 Lunch/Gr 7 ROCK 11:16 – 11:42 26 min.	Gr 8 Lunch/Gr 7 ROCK 11:25-11:51 26 min.
Gr 8 Lunch/Gr 7 ROCK 11:42 – 12:08 26 min.			Gr 8 Lunch/Gr 7 ROCK 12:00-12:26 26 min.	Gr 8 Lunch/Gr 7 ROCK 11:42 – 12:08 26 min.
Period 6 12:08 – 12:50 42 min.	Gr 8 Lunch/Gr 7 ROCK 12:26-12:52 26 min.	Gr 8 Lunch/Gr 7 ROCK 12:26-12:52 26 min.	Period 6 12:08 – 12:50 42 min.	Period 6 12:17 – 12:56 39 min.
Period 7 12:53 – 1:35 42 min.	Period 7 12:54 – 2:20 86 min.	Period 8 12:54 – 2:20 86 min.	Period 7 12:53 – 1:35 42 min.	Period 7 12:59 – 1:38 39 min.
Period 8 1:38 - 2:20 42 min.			Period 8 1:38 - 2:20 42 min.	Period 8 1:41 - 2:20 39 min.

HBMS Master Schedule Pilot

Three Objectives:

- Greater access to programs for all students:
 - greater opportunities for students in special education to participate in the general education curriculum
 - increase access to Read 180 for non-identified students
 - increase access to CORE teachers during skills (include in an actual skills class) for students in “off-team” math class
- Create greater equity for all professional staff members with individual plan and common plan time.
- Provide continuity of instruction by increasing seat time in core classes from three times per week to four.

Process:

1. June 2018: Special Education Program Evaluation conducted by NHASEA
2. October: Instructional Leadership Team begins review of current master schedule. Invitation to participate in the process is sent to all staff members.
3. November-December: Instructional Leadership Team researches alternative master schedules.
4. January: Representative group of staff members attend the New England League of Middle Schools conference on master schedule design. Staff members include: Steve Capraro, Patti Flynn, Carol Swanson, Liz Nault, Karen Coutu, Kirby Elliott, Jess Barrett, Amanda Delaney, Holly Babcock, Gina Bergskaug and Carol Tyler.
5. February: Construction of draft schedules.
6. March: Two draft schedules shared with all staff and reviewed at department meetings
7. April: Draft schedules submitted to building level administration for review.
8. May: Final draft submitted to SAU administration.

Teacher Schedule Breakdown

	Current Schedule for CORE teachers	Current Schedule for Specialist teachers	Proposed Master Schedule
Instructional Time	209 minutes Per Week	208 minutes per week	209 minutes per week
Individual Planning Time*	248 minutes for 2 quarters 456 minutes for 2 quarters	208 minutes for 2 quarters 406 minutes for 2 quarters	248 minutes for 2 quarters 456 minutes for 2 quarters
Common Planning Time	166 minutes	22 minutes per week	170 minutes per week
Duty Coverage	208 minutes for 2 quarter (allowed to do 3)	208 minutes for 2 quarters (allowed to do 3)	209 minutes for 2 quarters (allowed to do 3)

*Currently Core teachers have one 42 minute plan period per day and specialists have two 21 minute plan periods per day.

Contract Language:

Section 10.6 Middle School:

Full time Staff Members shall be assigned the equivalent of five (5) teaching periods per day. Each full-time staff member will be assigned to a skills period and/or tutoring students not to exceed one (1) period per day for the equivalent of three (3) quarters per year. Staff Members will be assigned to lunch duty, bus duty or another duty that is mutually acceptable to the building administrator and individual staff member and shall not exceed one (1) assignment for one (1) quarter.

One (1) of the two (2) preparation periods per day is designated for Common Planning Time (CPT) and Professional Learning Community (PLC) time. CPT will occur during four (4) of those preparation periods each week and PLC will occur during one (1) of those preparation periods each week.

Hollis Brookline Middle School Tech Center

Article 13. Because there is the possibility that Article 1 will be defeated, or that other considerations will result in the space created by Article 1 not being adequate or available for the HBHS Robotics Team, to see if the school district will vote to raise and appropriate the sum of ~~\$550,000~~ **\$98,311** for the purpose of funding a facility for the HBHS and HBMS robotics teams. ~~Funds to be transferred to the HB Robotics Boosters for this purpose~~ (Majority vote required). Submitted by Citizen Petition. The school board does not recommend this appropriation (0-6-0).

Room 103

- Current robotics room, ~1100 ft², 96 ft² storage room, door to Rm 104 (current science classroom)
- Return to science
 - Facilitate communication and collaboration with science teacher in Rm 104
 - Facilitate sharing of resources with Rm 104
- Will need:
 - New flooring
 - Furniture and equipment moved from current science classroom
 - SMART Board or additional whiteboard space

Rooms 105/106

- Current woodshop and Tech Ed classroom space, ~1250 ft² shop, 750 ft² classroom, 216 ft² storage
- Create shared space
- Will need:
 - Old tools removed/sold
 - Divider to separate teacher/robotics tools from general access
 - Student tool upgrade
 - Robotics tool upgrade
 - New door access between storage and shop
 - New door access between Rm 107 and shop
 - New key fob entrance
 - Storage units for shop and storage room
- Allows the curriculum to move forward
- Allows the space to be upgraded for safety and relevance

Room 107

- Current science classroom, 1152 ft², 56.25 ft² storage closet
- Create new robotics assembly space
- Will need:
 - New door access to shop (see above)
 - Cap gas lines
 - Pull down electric
 - Flexible tables/work spaces
 - Removal of cabinetry

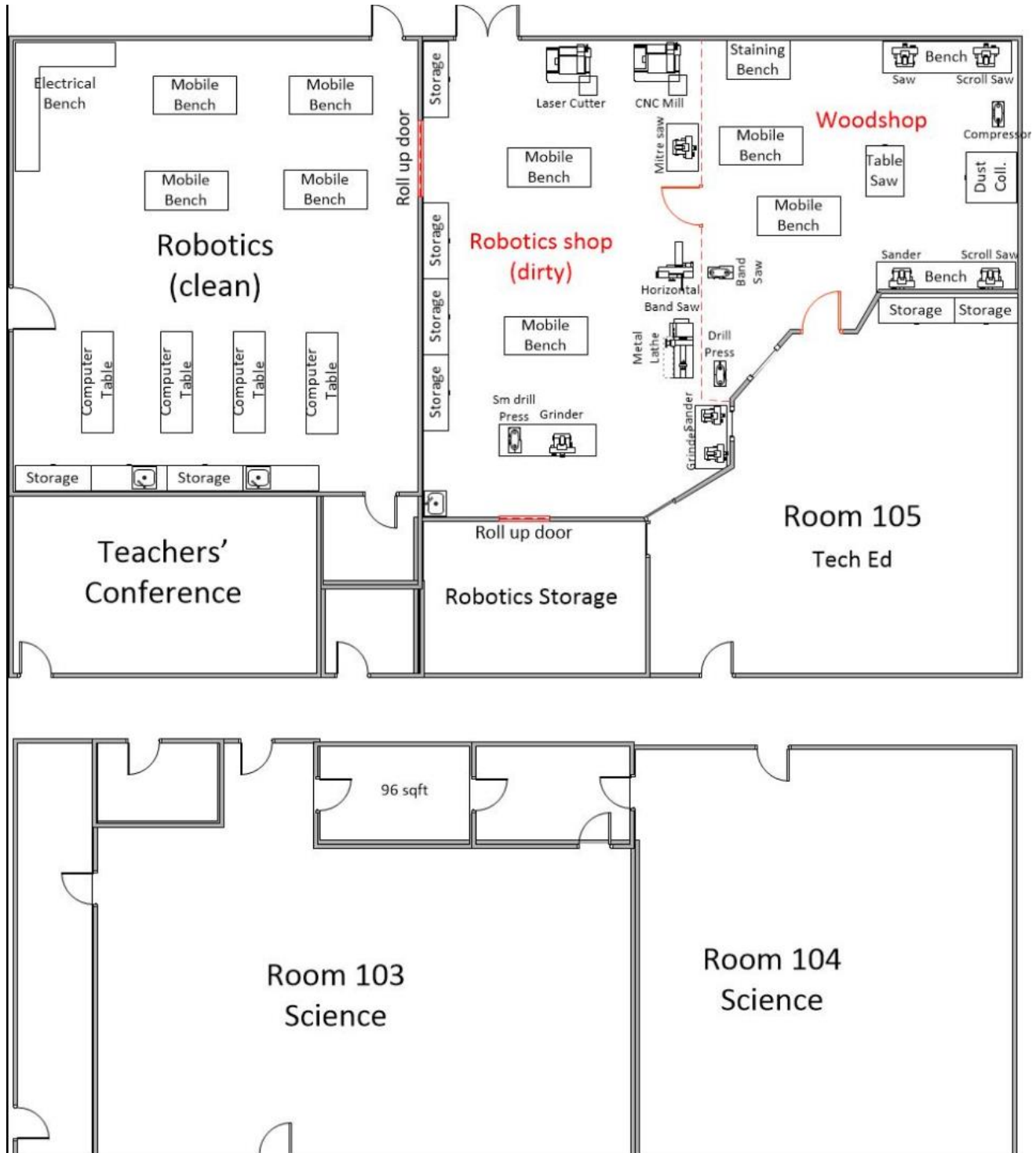
No Changes

- No changes proposed to North Conference room
- No changes to classrooms 109 and 110
- All three spaces to continue as shared spaces

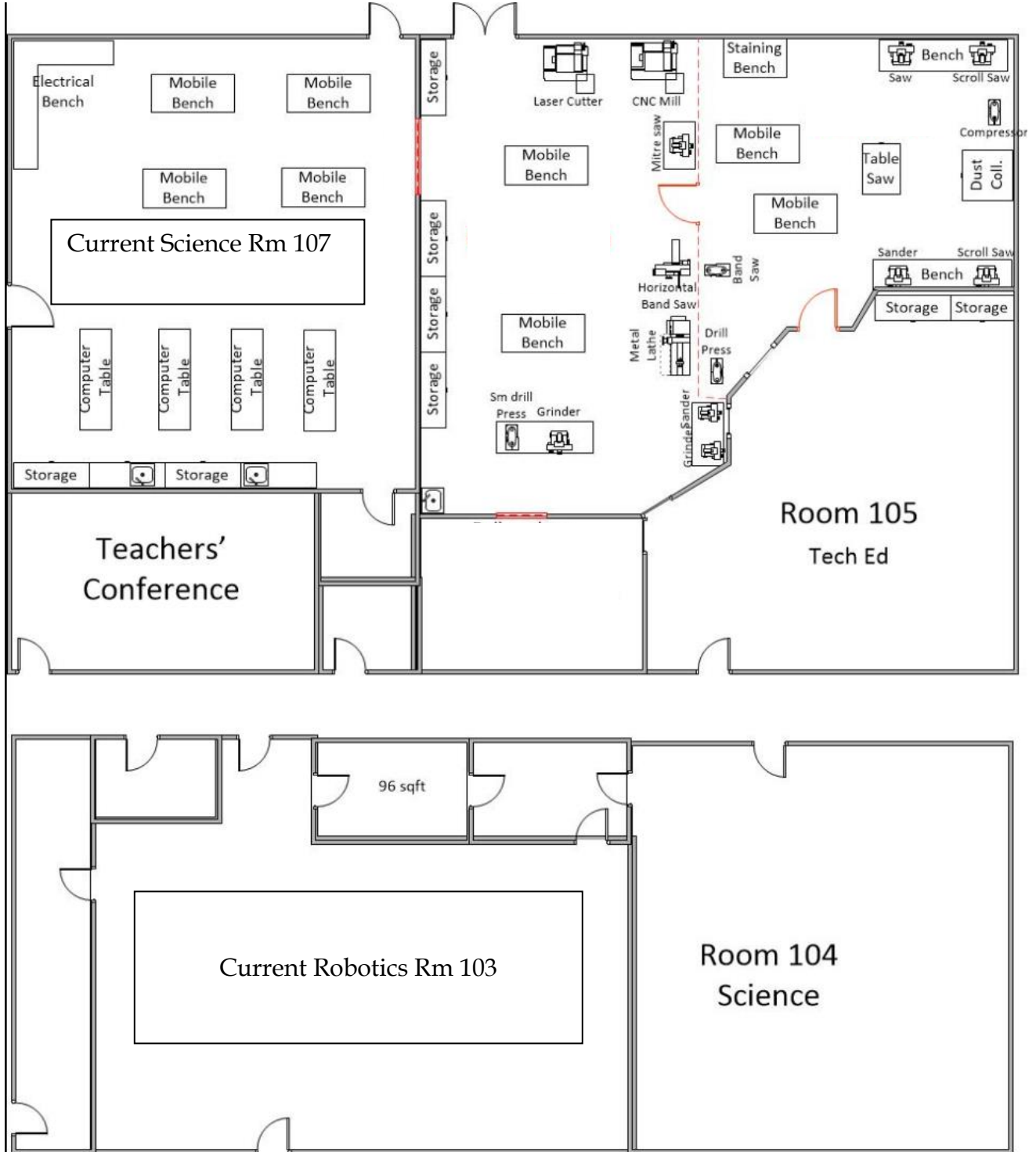
Curriculum

- Tech Ed Curriculum update in progress—bring new teacher and new principal into the mix
- Maintain wood shop & build aspect of tech ed
- Add additional technology to the design portion of the curriculum
- Potentially add features of Green Architecture
- Over time, ideally run the course with student choice for final outcome

Proposal



Current State



Scope and Sequence Technology Education

7-8 Scope & Sequence

	Unit 1	Unit 2	Unit 3
Grade 7	Introduction to Tools and Safety: Bridge		
Grade 8	Introduction to Tools and Safety: Sound Amplification		

Grade Level Scope & Sequence

Content Area:	Technology Education	Grade Level:	7, 45 days
Date Created:	April 2019	Author(s):	Bergskaug
Date Revised:		Author(s):	

Introduction
<p>Technology/engineering education is the discipline devoted to the study of human invention and innovation and their influence on our natural and human-made environment.</p> <p>https://www.education.nh.gov/career/career/documents/tech_ed_curr_guide.pdf</p>

	Unit 1	Unit 2	Unit 3	Add columns as needed
Unit Title	Introduction to Tools and Safety		Game	
Time: class periods/weeks	10	15	20	
Purpose: <i>Why is this topic and skill set important for students? Consider the value of the content...</i>	The purpose of this introductory unit is to introduce basic concepts of machinery and safety rules and regulations within the context of a design challenge.			
Goals & Outcomes: <i>In 2-4 sentences, describe the desired results for students to have by the end of the unit.</i>	Students will design and build a bridge to span a certain distance that can withstand a given stress (different for each group).			

<p><i>“Students will read/listen to ___ in order to ___”</i></p> <p><i>“Students will show learning by using writing and/or speaking to ___”</i></p>	<p>Students will listen to instruction relative to the safe operation of instrumentation and work together in a team with assigned team roles for the design, development, and modification of said device.</p>			
<p>Priority-Level Standards:</p> <p><i>List only the standards which will be explicitly taught and assessed.</i></p>	<p>A, B, C in tech ed curriculum guide</p>			
<p>Key Resources:</p> <p><i>List 2-3 authentic and relevant resources that students will read and/or listen to. Include tests, videos, etc.</i></p>	<ul style="list-style-type: none"> ● Equipment Safety Video ● Safety Standards Assessment ● Equipment Performance Assessment ● Bridge assessment ● Tools for design <p>https://www.education.nh.gov/career/career/documents/tech_ed_curr_guide.pdf</p>			

Grade Level Scope & Sequence

Content Area:	Technology Education	Grade Level:	8, 45 days
Date Created:	April 2019	Author(s):	Bergskaug
Date Revised:		Author(s):	

Introduction
<p>Technology/engineering education is the discipline devoted to the study of human invention and innovation and their influence on our natural and human-made environment.</p> <p>https://www.education.nh.gov/career/career/documents/tech_ed_curr_guide.pdf</p>

	Unit 1	Unit 2	Unit 3	Add columns as needed
Unit Title	Intro to Tools and Safety		Bowls	
Time: class periods/weeks	10	15	20	
Purpose: <i>Why is this topic and skill set important for students? Consider the value of the content...</i>	The purpose of this introductory unit is to introduce basic concepts of machinery and safety rules and regulations within the context of a design challenge.			
Goals & Outcomes: <i>In 2-4 sentences, describe the desired results for students to have by the end of the unit.</i> <i>"Students will read/listen to</i>	Students will design and build a device to amplify sound. Students will listen to instruction relative to the safe operation of instrumentation and work			

Scope

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

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

Regulatory Compliance

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

- Children’s Internet Protection Act ([CIPA](#))
- Children’s Online Privacy Protection Act ([COPPA](#))
- Family Educational Rights and Privacy Act ([FERPA](#))
- Health Insurance Portability and Accountability Act ([HIPAA](#))
- Payment Card Industry Data Security Standard ([PCI DSS](#))
- Protection of Pupil Rights Amendment ([PPRA](#))
- Individuals with Disabilities in Education Act ([IDEA](#))
- New Hampshire State RSA - Student and Teacher Information Protection and Privacy
 - [NH RSA 189:65](#) Definitions
 - [NH RSA 189:66](#) Data Inventory and Policies Publication
 - [NH RSA 189:67](#) Limits on Disclosure of Information
 - [NH 189:68](#) Student Privacy
 - [NH RSA 189:68-a](#) Student Online Personal Information
- [New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data](#)
- New Hampshire State RSA - Right to Privacy:

[NH RSA 359-C:19](#) - Notice of Security Breach Definitions

[NH RSA 359-C:20](#) - Notice of Security Breach Required

[NH RSA 359-C:21](#) - Notice of Security Breach Violation

Data User Compliance

The Data Governance Plan applies to all users of SAU41's information including: staff, students, volunteers, and authorized district contractors or agents. All data users are to maintain compliance with School Board Policies and District administrative procedures, EHAB (Data Governance and Security), GBEF (Employee Use of District-Issued Computers, Devices and the Internet, formally GCSA), GBEF-R (Employee Computer/Device and Internet Responsible Use Rules, formally GCSA-R), JICL (Student Use of Computers, Devices and the Internet, formally EGA), JICL-R (Student Technology Responsible Use, formally EGA-R) and all policies, procedures, and resources as outlined within this Data Governance Plan and School Board Policy.

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

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

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

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

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

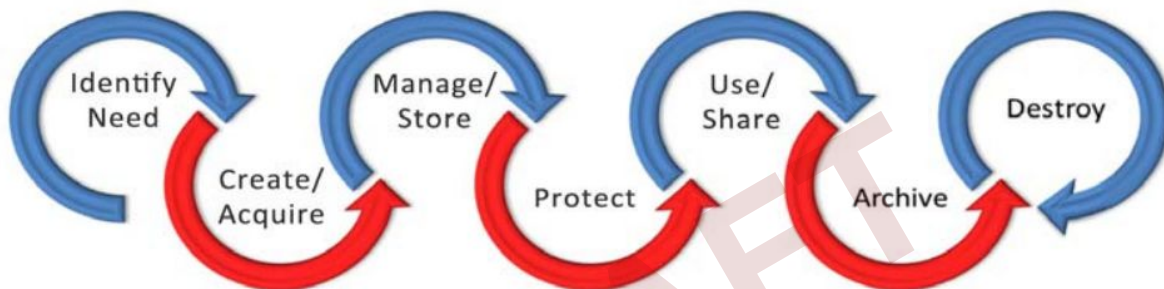
Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of PII or Confidential Information.
- Sharing your user IDs or passwords with others (exception for authorized technology staff for the purpose of support)
- Applying for a user ID under false pretenses or using another person's ID or password.
- Unauthorized use of an authorized password to invade student or staff privacy by examining records or information for which there has been no request for review.

- The unauthorized copying of system files.
- Attempting to secure a higher level of privilege without authorization.
- Installation or use of unlicensed software or software not approved for district systems.
- The intentional unauthorized altering, destruction, or disposal of district information, data and/or systems. This includes the unauthorized removal of technological systems such as but not limited to: laptops, internal or external storage, computers, security or video cameras, servers, backups or other media, that may contain PII or confidential information.
- The introduction of computer viruses, hacking tools or other disruptive or destructive programs.

Data Lifecycle

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



Identifying Need & Assessing Systems for District Requirements

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

New Systems

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

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

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

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

- Curricular value

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

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

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

Review of Existing Systems

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

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

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

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

Acquisition and Creation

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

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

Management and Storage

Systems Security

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

Data Management

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

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

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

accuracy and security of data.

- assist the ISOs in enforcing district policies and procedures regarding data management.

Data Classification and Inventory

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data is classified according to the most sensitive detail they include. Data recorded in several formats (ie. source document, electronic record, report) have the same classification regardless of format (see Appendix E: Data Classification Levels).

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

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

Security/Protection

Risk Management

A thorough risk analysis of all SAU41 School District's data networks, systems, policies, and procedures shall be conducted by an external third party or as requested by the Superintendent, ISOs or designee. An internal audit of District network security will be conducted annually by District Technology staff. This analysis shall be completed using the risk management steps outlined in the Data Security Checklist (Appendix D). The product of the risk analysis will be referred to as the risk assessment. The risk assessment shall be used to develop a plan to mitigate identified threats and risk to an acceptable level by reducing the extent of vulnerabilities.

Security Logs

The District will maintain a comprehensive list of critical system events that will be logged and monitored to ensure data security. These events will include, but are not limited to, access to critical systems and modification of critical data. When applicable, notifications will be established for critical event triggers.

Physical Security Controls

Technology telecommunication closets are housed in secure locations. Access authorization is assigned through the Network Administrator. In addition, access to areas in which information processing is carried out shall be restricted to only appropriately authorized individuals (see appendix G: Physical Security Controls).

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

Inventory Management

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

Virus, Malware, Spyware, Phishing and SPAM Protection

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

Electronic Access Security Controls

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

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

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

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

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

Staff Users

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

to the ISOs with a clear justification for access.

Contractors/Vendors

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

Password Security

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

Concurrent Sessions

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

Remote Access

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

Securing Data at Rest and Transit

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

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

Usage and Dissemination

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

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

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

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

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

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

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

DRAFT

Appendix B - Laws, Statutory, and Regulatory Security Requirements

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

COPPA: The Children's Online Privacy Protection Act regulates operators of commercial websites or online services directed to children under 13 that collect or store information about children. Parental permission is required to gather certain information.

<https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy>

FERPA: The Family Educational Rights and Privacy Act applies to all institutions that are recipients of federal aid administered by the Secretary of Education. This regulation protects student information and accords students specific rights with respect to their data.

<http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

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

<https://www.hhs.gov/hipaa/index.html>

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

<https://sites.ed.gov/idea/>

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

PPRA: The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.

<https://www2.ed.gov/policy//gen/guid/fpco/ppra/index.html>

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

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

[New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data](#)

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

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

DRAFT

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

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

Approved Digital Resources

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

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

Digital Resource Licensing/Use

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

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

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

Appendix D - Data Security Checklist

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

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

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

Data Security Checklist for District Hosted Systems

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

Data Security Checklist for Provider Hosted Systems

- Inventory and classification of data on system
- Types of potential threats (internal, external, natural, manmade, electronic and non-electronic)
- Contract, terms of service and privacy policy are current and meet district data security requirements
- Provider has adequate data security measures including data management and incident response
- Ability to ensure proper access controls including password security (ie- can district password requirements be enforced)
- Authentication methods (LDAP/Active Directory, Single Sign On, District managed account, user managed account)
- Server/system security patch frequency
- Ability to access from mobile devices
- Notification practices in the event of a system compromise or security breach

Appendix E - Data Classification Levels

Personally Identifiable Information (PII)

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

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

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

Confidential Information

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

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

Internal Information

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

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

Directory Information

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

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

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

Public Information

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

This information may be disclosed outside of the district.

DRAFT

Appendix F - Securing Data at Rest and Transit

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

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

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with a G Suite for Education account that provides unlimited storage. Users are responsible for all digital content on their district provided G Suite for Education Drive. When using cloud storage, staff must adhere to the following guidelines:

- Staff and students may not access cloud storage through third party applications outside of approved internet browsers and Google Drive App on Android & iOS. This will ensure that native operating systems do not replace cloud sharing security.
- Users need to be aware of default sharing settings on folders when they upload files. Users are required to limit sharing files to an as needed basis.
- Staff and students must ensure that any cloud storage providers used are approved by the district and meet district student data and data security standards.
- When exiting the district, students should responsibly copy their content to their own personal storage solution.
- When exiting the district, staff should ensure that they are only copying personal content that they created. Staff are prohibited from copying content that contains confidential information, student records or data.
- Data with personally identifiable information of staff or students may be posted to users' district provided Google Drive with appropriate security settings. Users may not post this data to other cloud sharing platforms without consent of district administration.
- Staff should never post any documents labeled classified, confidential, or restricted to any cloud storage including district provided Google Drive accounts without district approval.
- All users shall immediately report any cloud storage security problems of the district's technology resources to a teacher or administrator.
- Attempting to gain or gaining unauthorized access to cloud storage or the files of another is prohibited.
- As with other forms of district technology, district staff, students, and other G Suite for Education drive users have no expectation of privacy on data stored on this platform.

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

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

External Storage Devices

The term “External Storage Devices” is used to define all portable storage devices (including USB drives, rewritable CD/DVD, memory cards, and external hard drives) used by staff and students. While the district recognizes the advantages for staff and students to maintain information on these devices, users are strongly encouraged to rely on their district provided G Suite for Education Drive account for all storage needs. When using external storage devices, staff must adhere to the following guidelines:

- Users are responsible for all content on external storage devices that have been connected to district technology resources.
- Users must ensure that they will not introduce harmful software including computer viruses, malware, non-district approved software, or hacking tools to district technology resources.
- Users must ensure that the data will remain secure through appropriate encryption or password protection when transferring files containing PII or protected information to an external storage device. Users should only keep the information stored on the external device for the duration of the project, and then promptly remove.
- Staff should never transfer any documents labeled classified, confidential, or restricted to any external storage device.
- Staff should never transfer or create confidential data or student records on personal storage devices.

File Transmission Practices

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

Credit Card and Electronic Payment

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

- Never store cardholder data on district systems or in written form. All cardholder data may only be entered in secured payment systems approved by the district. Any cardholder data collected in written form must be shredded immediately after entry into approved system.
- The district will never maintain a data system for payment information. All payment information will be stored and processed by a 3rd party accessible through a secure portal.
- Never request cardholder information to be transmitted via email or any other electronic communication system.
- Payment information shall be entered directly into the approved payment system by individual making payment. If the individual is not able to directly input the payment, designated staff may gain verbal approval for the payment process either in person or via phone (after identification is verified). If verbal payment information is received, that information must be entered directly into the payment system and not written down during the process.

DRAFT

Appendix G - Physical Security Controls RRTask

The following physical security controls shall be adhered to:

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

Appendix H - Asset Management

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

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

Inventory

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

Disposal Guidelines

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

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

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

Methods of Disposal

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

Discard

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

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

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

Donation/Gift

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

DRAFT

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

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

Internet Filtering

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

Phishing and SPAM Protection

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

Security Patches

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

DRAFT

Appendix J - Account Management

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

Staff Accounts

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

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

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

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

Local/Domain Administrator Access

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

Remote Access

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

Contractors/Vendors

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

Financial System Security Roles

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

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

Special Education System

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

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

Health Software System

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

Food Services System

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

roles and permissions are in place to ensure that confidential information is only viewable by authorized staff. The established roles are as follows:

Security Roles

Web Roles

- Administrator
- Manager

Register Roles

- Administrators
- POS Cashier
- Manager

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

DRAFT

Appendix L - Password Security

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

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

District network access to resources managed through LDAP

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

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

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

Appendix M - Technology Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable SAU41 (SAU41) to respond effectively and efficiently to a natural disaster or critical failure of the district's data center and/or core systems. The objectives during a natural disaster or critical failure are the following:

- Minimize the loss or downtime of core systems and access to business critical data.
- Recover and restore the district's critical systems and data.
- Maintain essential technology resources critical to the day to day operations of the district.
- Minimize the impact to the staff and students during or after a critical failure.

Planning Assumptions

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

- There may be natural disasters that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a disaster.
- There is the possibility of complete loss of the current data center.
- We will utilize existing storage to recover systems.
- District data is housed at district data centers and backed up in the cloud.
- District data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

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

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

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

Activation

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

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

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

Notification

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

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

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

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

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

Implementation

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

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

Deactivation

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

Evaluation

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

DRAFT

Appendix N - Data Breach Response Plan

Objectives

The purpose of the Technology Data Breach Plan (TDBP) is to enable SAU41 (SAU41) to respond effectively and efficiently to an actual or suspected data breach involving personally identifiable information (PII), confidential or protected information, district identifiable information and other significant cybersecurity incident. The objectives of the TDBP are:

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

Planning Assumptions

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

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

Data Breach/Incident Response Team

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

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

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

Activation

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

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

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

Notification

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

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

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

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

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

Implementation

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

- Data inventory of all systems containing sensitive data. A hard copy of this document will be secured at the technology office. An electronic version will be housed on the Technology Departments Team Drive.
- Data dictionary of all district hosted information systems. A hard copy of this document will be secured at the technology office. Due to non-disclosure agreements, this data may not be available in other locations/formats. The appropriate vendor(s) can be contacted for this information.
- Maintained spreadsheet listing all server names, physical and virtual, and their function. An electronic version will be housed on the Technology Information Team Drive.
- Maintained secure document to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.
- The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and offsite.

The following will take place during the incident response:

- The members of the IRT will be assembled once a breach has been validated. The IRT will be comprised of the Network Administrator, Database Manager, Assistant Superintendent, Business Administrator. Additional members of SAU41's administrative team and technology department may be designated to assist on the IRT.
- The IRT will determine the status of the breach, on-going, active, or post-breach. For an active and ongoing breach, the IRT will initiate appropriate measures to prevent further data loss. These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.
- The IRT will work with the data managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
- The IRMs will work with legal counsel and the Superintendent's Leadership Team to determine appropriate course of action pursuant to state statute. This includes notification of the authorities, and local law enforcement.
- Collaboration between the authorities and the IRT will take place with the IRMs. The IRT will work with the proper authorities to make sure any and all evidence is properly handled and preserved.
- On advice from legal counsel, an outside party may be hired to conduct the forensic investigation of the breach. When the investigation has concluded, all evidence will be safely stored, recorded or destroyed (where appropriate).
- All affected data, machines and devices will be identified and removed from the network as deemed appropriate for the investigation. Interviews will be conducted with key personnel and facts of the incident will be documented and the evidence preserved for later examination.
- The IRT will work with the Superintendent's office to outline the notification of the data owners and

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

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

Deactivation

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

Evaluation

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



STATUS REPORT: SAU41 & SB1612

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

HB 1612 Signed by Governor Sununu June 18, 2018

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

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

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

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

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

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

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

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

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

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

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

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



Per HB1612, inventoried, reviewed and vetted existing software applications

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

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

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

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

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

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

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

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

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

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

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

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



Compiled and distributed an inventory of all district software

Unlicensed Software

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

Developed Protocols for Protection of Student Data

Some resources require logins

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

How do we communicate our practices

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



Conducted Mandatory Student Privacy and Data Security Trainings in June 2018



SAU41

STUDENT PRIVACY & CLOUD TRAINING

TRAINING!!! MANDATORY FOR ALL!

Training Included:

Cloud-Based Software Criteria

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

Guidelines for Data Privacy and Security

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

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

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





SAU 41 Technology Initiative Approval Request *Cloud Based Software Services*

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

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

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

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

3. Does it require student information to be uploaded? Please be specific as to what student information will be uploaded. Place X next to all that apply.										
<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none;"><input type="checkbox"/> PowerSchool ID -</td> <td style="width: 50%; border: none;"><input type="checkbox"/> Date of Birth</td> </tr> <tr> <td style="border: none;"><input type="checkbox"/> Last Name (powerschoolid) -</td> <td style="border: none;"><input type="checkbox"/> Home Room</td> </tr> <tr> <td style="border: none;"><input type="checkbox"/> First Name</td> <td style="border: none;"><input type="checkbox"/> Password</td> </tr> <tr> <td style="border: none;"><input type="checkbox"/> Grade Level</td> <td style="border: none;"><input type="checkbox"/> Student Email</td> </tr> <tr> <td style="border: none;"><input type="checkbox"/> School</td> <td style="border: none;"><input type="checkbox"/> Other (Indicate the information)</td> </tr> </table>	<input type="checkbox"/> PowerSchool ID -	<input type="checkbox"/> Date of Birth	<input type="checkbox"/> Last Name (powerschoolid) -	<input type="checkbox"/> Home Room	<input type="checkbox"/> First Name	<input type="checkbox"/> Password	<input type="checkbox"/> Grade Level	<input type="checkbox"/> Student Email	<input type="checkbox"/> School	<input type="checkbox"/> Other (Indicate the information)
<input type="checkbox"/> PowerSchool ID -	<input type="checkbox"/> Date of Birth									
<input type="checkbox"/> Last Name (powerschoolid) -	<input type="checkbox"/> Home Room									
<input type="checkbox"/> First Name	<input type="checkbox"/> Password									
<input type="checkbox"/> Grade Level	<input type="checkbox"/> Student Email									
<input type="checkbox"/> School	<input type="checkbox"/> Other (Indicate the information)									

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

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

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

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

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

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

Staff Member: _____ Date: _____

Principal: _____ Date: _____

For SAU Office Use Only
Approval Request Process: Date Received _____ Initials _____
Committee Meeting Date: _____ Approved: <input type="checkbox"/> Yes <input type="checkbox"/> No Date: _____ Reason if not approved: _____
Signatures once approved/disapproved: Business Administrator _____ Date: _____ Network Administrator _____ Date: _____ Assistant Superintendent _____ Date: _____

Student Data

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

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

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

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

- (a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use.
- (b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed standards set by the department.
- (c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools and extensions.
- (d) A response plan for any breach of information.
- (e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

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

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

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





CLICK
HERE

SAU41 School Districts

Hollis and Brookline, New Hampshire

Search Site

Administration

SAU 41

Districts

Curriculum

Contacts

Resources

Quick Links

Business Office

Food Services

Human Resources

Information Technology

Student Services

Superintendent

Schools in SAU 41

Captain Samuel Douglass Academy

8:35am-3:10pm [Menu](#) [Bus Route](#) [Calendar](#)

Hollis Brookline High School

7:40am-2:30pm [Menu](#) [Bus Route](#) [Calendar](#)

Hollis Brookline Middle School

7:35am-2:20pm [Menu](#) [Bus Route](#) [Calendar](#)

Hollis Primary School

8:23am-3:05pm [Menu](#) [Bus Route](#) [Calendar](#)

Hollis Upper Elementary School

8:30am-3:00pm [Menu](#) [Bus Route](#) [Calendar](#)

Richard Maghakian Memorial School

8:25am-3:00pm [Menu](#) [Bus Route](#) [Calendar](#)





SAU41 School Districts

Hollis and Brookline, New Hampshire

Q Search Site

Administration

SAU 41

Districts

Curriculum

Contacts

Resources

Quick Links

SAU41 Software List

Reports

How-To Guides

Technology Policies

Live Stream

Information Technology

Schools in SAU 41 promote the integration of digital tools that support classroom teaching, strengthen student learning, increase student engagement, and assist students' development of digital literacy and digital citizenship capabilities.

Technology Use and Student Privacy

The SAU41 School District is committed to student privacy using best practices in our management of student information in accordance with the Family Educational Rights and Privacy Act (FERPA).

The SAU41 School District will not share personally identifiable information with third party software providers unless there is a valid educational interest for students. The SAU41 School District has implemented a best practice protocol for reviewing new online resources for potential use within the District. Only online websites and tools that are deemed appropriate in meeting instructional goals, as well as adhere to legal requirements protecting student privacy and data will be approved for use by students. More information on this process can

Helpful Links

[SAU 41 Software List](#)

[SAU 41 AUA](#)

[FERPA for Parents and Students \(US DOE\)](#)

[Student Privacy 101 \(US DOE\)](#)

[SAU 41 Technology Plan](#)



SAU 41 Software List

SAU41 Software						
Used by Brookline	Used by Hollis	Used by COOP	Name of Service / Software	Description	Publisher Website	Privacy S
		7-12	Adobe Creative Suite	Software suite of graphic design, video editing, and web development applications	http://www.adobe.com	installed k
K-6	K-6	7-12	AESOP	Substitute and Absence Management System	https://www.aesoponline.com	http://www.s/Privacy_
	K-6		AIMS Web	Benchmarking Assessment and Progress Monitoring tool	https://aimsweb.pearson.com/	
K-6	K-6	7-12	Alert Solutions	School Notification System	https://www.alertsolutions.com/	https://www.policy/
K-6	K-6	7-12	AppliTrack	Human Resource Employment Application System	http://www.applitrack.com/sau25/onlineapp/	http://www.s/Privacy_
	K-6		Brain Pop/BrainPop Jr.	Online interactive curriculum content	https://www.brainpop.com/	https://www._policy/
		9-12	Career Cruising	A self-exploration and planning program that helps people of all ages achieve their potential in school, career and life.	https://public.careercruising.com/en/	https://putacy-policy
4-6	4-6		Defined Stem	Project-based learning solution that providing lessons built around careers.	www.definedstem.com	https://www
K-6	K-6	7	Destiny	Library Automation and Resources	http://destiny.sau25.net	hosted int

CLICK HERE

CLICK HERE

[Licensed Software](#)

[Free Tools/Websites](#)

[Curricular Resources](#)

[Chrome Extensions](#)

[Paid Library Databases](#)

* Approved with expressed parent permission



Data Governance Plan

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

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

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

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

- (a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use.
- (b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed standards set by the department.
- (c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools and extensions.
- (d) A response plan for any breach of information.
- (e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

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

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

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

Data Governance Plan Development

Data Governance Team

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

Define Data Lifecycle & Data Security

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



Data Governance Plan

Plan for Critical Incident Response

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

Policy Work

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

Next Steps

Tackling the Requirements

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

Ongoing Work...

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

ACA

FREEDOM FROM SEXUAL HARASSMENT

POLICY:

It is the policy of the Hollis-Brookline School Board that all employees and students in the School District should be able to work and study in an environment that is free of sexual discrimination and sexual harassment.

PROCEDURE:

Procedures for prompt corrective action through mediation and persuasion and, when necessary, through discipline consistent with due process are considered to be an essential part of the District's effort to eliminate sexual harassment in all educational environments.

Building Principals, Assistant Principals and Supervisors are urged to take appropriate steps to distribute this policy statement and to inform employees and students of procedures for lodging complaints. Any employee or student having a complaint of sexual harassment should notify the Building Principal.

At any time, an employee or student and/or his representative may contact the Building Principal, Superintendent of Schools or a School Board member for counseling or advice.

Procedures for reporting are outlined in GBAA Section III.

Individuals shall not be reprimanded or discriminated against in any way for initiating an inquiry or complaint. The rights of an individual against whom a complaint is brought will also be protected.

The Freedom from Sexual Harassment Policy, formal and informal complaint procedures and names of complaint manager(s) shall be widely disseminated throughout the District's schools.

SANCTIONS:

Sexual harassment will be treated as a major disciplinary offense so that, depending upon the circumstances and the degree of harassment, the offender(s) might be disciplined with a suspension subject to discharge.

APPEAL BOARD

The Hollis-Brookline School Board, upon receipt of notification of ~~the Superintendent-the grievance officer or complaint manager~~, shall ~~serve as the Appeal Board~~ appoint a five member appeal board. One member shall be a parent or guardian of a student of the district; one member shall be a teacher employed by the District; one member shall be selected from the School

~~Board; one member shall be selected from the public; and one member shall be a principal from a District school. In the event any member would be disqualified to act as a juror in any matter referred to it the Board shall appoint an alternate from the same category as the disqualified member.~~

~~The Appeal Board shall hold an informal hearing to hear the complaint within 30 days of the receipt of the matter. Within 10 days after the hearing, the Appeal Board shall make its recommendations to the School Board. Such recommendations shall be in writing with copies provided to all parties involved in the appeal procedure.~~

~~The School Board may affirm, modify or reject the report of the Appeal Board no later than its second regular meeting after the receipt of the Appeal Board's report. The School Board will hold an informal hearing to hear the complaint. The School Board will make a determination in a reasonable amount of time. The School Board's determination shall be final.~~

Any inquiries, complaints, grievances, and other communication relative to the policy and to Title IX and the applicable federal regulations are to be made to the Title IX Coordinator and/or the Superintendent of Schools.

The following person has been designated to handle inquires regarding Title IX:

The Building Principal or designee as determined by the Superintendent of Schools.

May 19, 2019 First Read

June 19, 2019 Second Read

Formatted: Font: Italic

Category: Priority/Required by Law

Related Policies [EHAA](#), [EHB](#), [GBEBD](#), [GBEF](#), [IHBH](#), [JICJ](#), [JICL](#), [JICM](#), [KD](#), & [KDC](#)

DATA GOVERNANCE AND SECURITY

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

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

A. Definitions

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

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

B. Data and Privacy Governance Plan - Administrative Procedures.

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

The Data Governance Plan shall include:

- (a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use;
- (b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed minimum standards set by the New Hampshire Department of Education;

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

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

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

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

C. Information Security Officer.

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

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

D. Responsibility and Data Stewardship.

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

E. Data Managers.

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

F. Confidential and Critical Information.

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

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

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

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

G. Using Online Services and Applications.

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

H. Training.

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

I. Data Retention and Deletion.

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

J. Consequences

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

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

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

Legal References:

*15 U.S.C. §§ 6501-6506 * Children's Online Privacy Protection Act (COPPA)*

*20 U.S.C. § 1232g * Family Educational Rights and Privacy Act (FERPA)*

*20 U.S.C. § 1232h * Protection of Pupil Rights Amendment (PPRA)*

*20 U.S.C. § 1400-1417 * Individuals with Disabilities Education Act (IDEA)*

*20 U.S.C. § 7926 * Elementary and Secondary Education Act (ESSA)*

*RSA 189:65 * Definitions*

*RSA 186:66 * Student Information Protection and Privacy*

*RSA 189:67 * Limits on Disclosure of Information*

*RSA 189:68 * Student Privacy*

*RSA 189:68-a * Student Online Personal Information*

*RSA 359-C:19-21 * Right to Privacy/Notice of Security Breach*

District Policy History:

First reading: June 12, 2019