Hollis Brookline Cooperative School Board
Wednesday, May 15, 2019
Hollis Brookline Middle School Library
All times are estimates and subject to change without notice

6:00 Call to Order

6:05 Appointment of a process observer
Agenda adjustments
Approve meeting minutes
Nomination/ resignations/retirements/correspondence

6:15 Public Input

6:30 Principal Reports/Athletic Report

6:50 Non – Public Session under RSA 91-A: 3II (a) Compensation and/or (c) reputation

7:50 Discussion

- Facilities Committee update – Field update – Superintendent Corey
- Revenue and Expense Update – Linda Sherwood
- MS Master schedule update – Principal Thompson, Assistant Superintendent Bergskaug
- Curriculum Discussion – Tech Education - Assistant Superintendent Bergskaug
- Data Governance Plan – Carol Tyler

8:45 **Deliberations**

- To see what action the Board will take regarding the Superintendent's recommendation(s) for non –union and administrative compensation
- To see what action the Board will take regarding the Middle Schools' administrations recommendation of the master schedule
- To see what action the Board will take regarding the Board Chair signing the General Assurances Requirements
- To see what action the Board will take regarding policy ACA – Freedom from Sexual Harassment – first reading
- To see what action the Board will take regarding - policy ILD -Educational Questionnaires, Surveys and Research - second reading.
- To see what action the Board will take regarding - policy ADC-Tobacco Products Ban - second reading
- To see what action the Board will take regarding - policy AC - Non-discrimination - second reading
- To see what action the Board will take regarding - policy IJOC - Volunteers - third reading

9:15 Motion to Adjourn

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

Informational

Performing Arts: Congratulations to **Amy Norton '19**, who was recently recognized for *the third straight year* for her annual entries into the NHMEA Composition Competition, and has been selected as a 2019 winning composer by *DownBeat* magazine. *DownBeat* is the preeminent jazz periodical and has been announcing student awards for forty-two years. Amy's piece, "Ecuador," was the winning original composition for large ensemble in the high school category. The student awards will be published in the June issue. Congratulations to Amy on this enormous honor!

First Robotics: Congratulations to Team 1073 for their **3rd place finish at World Championships** in Detroit over the break! This event included over 400 of the best teams out of the nearly 4000 teams in the world. The team entered the division finals as the fourth seeded alliance, easily won in the first round, and then in the second faced the number one seeded alliance that included the two teams from Ontario that were the championship favorites and generally recognized as the best two teams in the world this year. With a well-designed robot, great teamwork, awesome work by our mechanical students in the pit, Team 1073 prevailed! They then went on to win the division and advance to the finals. This is the first time that 1073 *has ever* won a division at Worlds and the first time in years that a team from New Hampshire has done it.

Congratulations to **Cam Hallett '20** was chosen as 1 of 10 students worldwide to win the FRC Deans List Award. This is a significant honor and includes scholarships and lifelong opportunity.

Congratulations to Team 1115 from Hollis which consists of **Peter '19** and **Steven Szczeszynski '20** who also competed in Detroit and won first place in the Technical Challenge Division.

Journalism Award: Congratulations to **Hannah Riseman '20** who was chosen to be the NH representative of the " Al Neuharth Free Spirit and Journalism Conference! This annual program

targets rising high school seniors who are interested in pursuing a career in journalism and who demonstrate qualities of “free spirit.”

Students **will come to Washington, D.C. June 14-20, 2019**, to participate in an all-expenses-paid journalism conference at the Newseum, located at 555 Pennsylvania Ave., NW and are **awarded a $1,000 college scholarship**. This Freedom Forum Institute program was established in 1999 to honor Al Neuharth, the founder of *USA Today*, Newseum and the Freedom Forum. The conference is designed to inspire and encourage students to pursue journalism."

Guitar Night: The annual community event was a tremendous success. Thanks to the club advisors Mr. and Mrs. Perry who went above and beyond as they provide space for seasoned performers and those who have ever sang in front of a live audience. It is an incredibly valuable opportunity for our students.

Respectfully Submitted,

Rick Barnes
Principal

To: Hollis Brookline Cooperative School Board
From: Bob Thompson, Principal HBMS
Re: Principal's Report
Date: May 15, 2019, Scheduled Meeting

INFORMATION ONLY

Empty Bowls - On Monday, May 20th, Hollis Brookline Middle School's 7th Annual Arts Night/Empty Bowls event is a celebration of our students' achievements in the performing and visual arts! In addition, Empty Bowls is an opportunity for our students to learn about hunger and poverty in America as well as in our own towns of Hollis and Brookline. Each student has created a unique, handcrafted wool felted bowl to be donated and later purchased at the event. We will also have a collaborative fiber arts piece, designed and constructed by Hollis Brookline High School's National Art Honor Society students. Our "gymnasium exhibit" will highlight our skillful HBMS student artists' paintings, drawings and sculptures.

National History Day – Seven students from the HBMS National History Day Club (NHD) have qualified for the National Competition. The National Contest is the final stage of a series of contests at local and state/affiliate levels. Students begin their journey by presenting their projects in classrooms, schools, and districts around the world. Top entries are invited to the state/affiliate level contests. The top two entries in every category at the state/affiliate level are then invited to the National Contest. The 2019 National Contest will be held from June 9 - 13, 2019, at the University of Maryland, College Park. Congratulations to Katherine B., Gabriella R., Madi L., Bethany C., Anneli D., Ivy R. and Caitlyn M. A special thank you is in order to Sue Connolly who serves as the advisor to the club.

Letters about Literature - 8th grade students Daniella A. and Owen J. were named level 2 (grades 7 and 8) semifinalists for the Letters About Literature Contest. Letters About Literature is a writing contest sponsored by the Center for the Book in the Library of Congress. Students are asked to write to a favorite author describing how that author's work changed the reader's view of the world.

HBMS Leadership Transition - The transition to a new principal at HBMS is well underway. Mr. Girzone has had the opportunity to visit HBMS on several occasions. During his time he has helped conduct interviews for both Tech Ed and Spanish hiring. He has had the opportunity to meet with staff members. Discussions are currently underway regarding budget, schedule, students and various operational components of the school. Additionally, last month Mr. Girzone traveled with the current administrative team to both CSDA and HUES to meet with the current 6th grade class as part of their transition to middle school. Mr. Girzone has several more visits planned between now and July 1st.

HBMS Chorus - On May 21st at 6:00 p.m. the HBMS chorus will perform the National Anthem at the Fischer Cats Game. Tickets for this fun event can be ordered at:

https://docs.google.com/viewer?a=v&pid=sites&srcid=c2F1NDEub3JnfGhibXMtYmFuZHxneDozODU5ODA2Zjk4MTY4MTE5

Important Dates:

May 14 - Hollis Brookline School District Band Concert 7:00-8:30 p.m. HBHS
May 20 - Arts Night/Empty Bowls 6:00 p.m. HBMS
May 21 - HBMS Chorus Sings National Anthem at Fischer Cats Game 6:00 p.m.
June 19 - Tentative Date for 8th Grade Canobie Lake Trip

To: Andrew Corey, Superintendent
From: Brian Bumpus, District Athletic Coordinator
Re: May 2019 Board Report

HBHS Spring Sports: Spring teams are well into their seasons at this point, and several of them are poised to make deep play-off runs. Currently, the HBHS Boys and Girls Lacrosse teams, along with the Boys Tennis team, are undefeated and sit atop their respective standings. The Baseball team sits in 2nd place overall, while the Softball and Boys Volleyball teams are both ranked in the top half of their divisions and are in position to host at least a 1st round tournament game. The Outdoor and Unified Track teams have had impressive seasons up to this point as well, with the Unified Track team hosting their first ever home meet on May 8th.

HBMS Spring Sports: The inaugural season for Lacrosse at HBMS is off to a great start, with the boys and girls teams currently sitting at 2-2 and 3-1, respectively. The Baseball and Softball teams are also off to a strong start, with records of 3-2 for both teams. All four teams are poised to make their Tri-County tournaments, as play-offs are right around the corner. The HBMS Track team this year has three new coaches, who have done a wonderful job organizing 62 student-athletes into many different events. HBMS hosted a home meet on May 2nd, and with the help of many people throughout the district, it went extremely well!

Community Service: In an effort to give back to the community, the HB Athletic Booster Club has initiated several community service opportunities for our athletic teams to take part in over the past few months. During the Hollis Town Meeting, held at Hollis Brookline High School, the HBHS Cheer team donated their time to babysit throughout the day. More recently, the HBHS Outdoor Track team participated in a clean-up day in preparation for the Hollis Fast 5K road race (photos below). We look forward to working with the Booster Club to expand this initiative and provide more opportunities to teams across the district to give back.

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

Golf Head Coach (HBHS)

Cross Country Head Coach (HBHS)

Cross Country Asst. Coach (HBHS)

Bass Fishing Head Coach (HBHS)

Boys Reserve Soccer Head Coach (HBHS)

Skiing Head Coach (HBHS)

Skiing Asst. Coach (HBHS)

Respectfully Submitted,

Brian Bumpus
District Athletic Coordinator

Hollis Brookline Cooperative School District

FY19 YTD Expense and Revenue Report

Expenses as of 5/7/2019

Description	Budget	YTD Expense	Encumbered	Balance
Regular Education	$ 5,701,951	$ 4,225,791	$ 1,447,506	$ 28,654
Special Education	$ 3,482,433	$ 2,653,879	$ 735,077	$ 93,477
Vocational Program	$ 40,840	$ 16,305	$ 17,808	$ 6,727
Co-curricular Program	$ 748,177	$ 583,701	$ 150,668	$ 13,808
Student Support Services	$ 1,387,377	$ 934,902	$ 421,860	$ 30,616
Instructional Staff Support	$ 703,406	$ 431,597	$ 173,405	$ 98,404
*School Board/SAU Assessment	$ 977,608	$ 783,146	$ 101,791	$ 92,672
School Administration	$ 1,076,405	$ 908,196	$ 149,102	$ 19,107
Facilities	$ 1,274,582	$ 1,059,561	$ 169,879	$ 45,142
Transportation	$ 1,123,522	$ 927,440	$ 271,997	$ (75,915)
Benefits	$ 4,740,915	$ 3,606,167	$ 1,127,824	$ 6,925
Site improvements	$ 75,500	$ 70,418	$ 941	$ 4,142
Debt Service	$ 620,191	$ 595,867	$ -	$ 24,324
Transfers	$ 2,474,000	$ 1,816,133	$ 654,000	$ 3,868
TOTAL	**$ 24,426,907**	**$ 18,613,100**	**$ 5,421,858**	**$ 391,949**
FY18 Expense Carryover	$152,203	$119,401	$21,474	$11,328
TOTAL FY18 + FY19	**$ 24,579,110**	**$ 18,732,501**	**$ 5,443,332**	**$ 403,277**

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

Revenue as of 5/7/2019

Description	Budget	YTD Revenue	Expected	Balance
Local Property Tax	$ 15,295,661	$ 14,770,000	$ 525,661	$ -
Adequacy Aid Grant/Tax	$ 5,157,701	$ 3,016,549	$ 2,141,152	$ -
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	$ 59,866	$ 200,134	$ -
Food Service	$ 38,000	$ 38,000		$ -
Medicaid	$ 146,457	$ 67,459	$ 58,998	$ (20,000)
Local				$ -
Tuition	$ 5,000	$ 7,353		$ 2,353
Food Service Sales	$ 353,000	$ 325,467	$ 27,533	$ -
Other	$ 5,000	$ 93,913		$ 88,913
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**	**$ 21,089,854**	**$ 3,416,204**	**$ 79,151**

Total Expense Balance	**$403,277**
Total Revenue Balance	**$79,151**
Unreserved Fund Balance	**$482,428**

Anticipated Reductions to Unreserved Fund Balance

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

Fund Balance Returned to Taxpayers **$73,428**

Explanation of budget balances on current expense report

5/7/2019

Function	Description	Current Balance	Notes
1100	**Regular Education**	$ 28,654	Staffing changes; fewer lane changes than expected
1200	**Special Education**	$ 93,477	Savings in salaries, OOD tuition, tutoring, and services
1300	**Vocational Program**	$ 6,727	Lower # of voc ed students than budgeted
1400	**Co-curricular Program**	$ 13,808	Some athletic assistant stipends not filled; lower academic competition fees
2100	**Student Support Services**	$ 30,616	Savings in consultations
2200	**Instructional Staff Support**	$ 98,404	Savings in teacher professional development and MLP reimbursements
2300	**chool Board/SAU Assessment**	$ 92,672	$100K contingency fund not being used
2400	**School Administration**	$ 19,107	Savings in service agreements and replacement equipment
2600	**Facilities**	$ 45,142	Savings in custodial salaries due to unfilled positions and in snow removal
2700	**Transportation**	$ (75,915)	Vocational Education transportation-- lease of vans postponed
2900	**Benefits**	$ 6,925	Higher health and dental insurance due to open enrollment choices
4000	**Site improvement**	$ 4,142	
5100	**Bonds**	$ 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	$ 391,949	

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	Bonds	Principal and interest payments on bonds
5200	Transfers	Accounting line to make total expenses match total revenue, and match the budget.

HBMS Bell Schedule 2019 – 2020

Monday	Tuesday (Odd Day)	Wednesday (Even Day)	Thursday	Friday with PLCs
Period 1 7:35 – 8:17	**Period 1** 7:35 – 09:01	**Period 2** 7:35 – 09:01	**Period 1** 7:35 – 8:17	**Period 1** 8:00 – 8:39
Period 2 08:20 – 9:02			**Period 2** 08:20 – 9:02	**Period 2** 08:41 – 9:20
Period 3 9:05 – 9:47			**Period 3** 9:05 – 9:47	**Period 3** 9:23 – 10:01
	Period 3 09:04 – 10:30	**Period 4** 09:04 – 10:30	**Period 4** 9:50 – 10:31	
Period 4 9:50 – 10:31	**Period 5** 10:33 – 11:59	**Period 6** 10:33 – 11:59		**Period 4** 10:04 – 10:43
Period 5 10:34 – 11:16			**Period 5** 10:34 – 11:16	**Period 5** 10:46 – 11:25
Lunch & ROCK 11:16 – 12:08 **Gr 8 Lunch/Gr 7 ROCK** 11:16-11:42 **Gr 7 Lunch/Gr 8 ROCK** 11:42-12:08	**Lunch & ROCK** 12:00 – 12:52 **Gr 8 Lunch/Gr 7 ROCK** 12:00-12:26 **Gr 7 Lunch/Gr 8 ROCK** 12:26-12:52	**Lunch & ROCK** 12:00 – 12:52 **Gr 8 Lunch/Gr 7 ROCK** 12:00-12:26 **Gr 7 Lunch/Gr 8 ROCK** 12:26-12:52	**Lunch & ROCK** 11:16 – 12:08 **Gr 8 Lunch/Gr 7 ROCK** 11:16-11:42 **Gr 7 Lunch/Gr 8 ROCK** 11:42-12:08	**Lunch & ROCK** 11:25 – 12:17 **Gr 8 Lunch/Gr 7 ROCK** 11:25-11:51 **Gr 7 Lunch/Gr 8 ROCK** 11:51-12:17
Period 6 12:08 – 12:50	**Period 7** 12:54 – 2:20	**Period 8** 12:54 – 2:20	**Period 6** 12:08 – 12:50	**Period 6** 12:17 – 12:56
Period 7 12:53 – 1:35			**Period 7** 12:53 – 1:35	**Period 7** 12:59 – 1:38
Period 8 1:38 - 2:20			**Period 8** 1:38 - 2:20	**Period 8** 1:41 - 2:20

Hollis Brookline Technology and Engineering Program

Ed 306.47 Technology/Engineering Education Program.

(a) 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.

(b) The local school board shall require that a technology/engineering education program in each middle school provides:

(1) Opportunities for students to develop an understanding of the technological world in which they live and will someday work;

Accomplished through rich curriculum utilizing hands-on, project-based assessments.

(2) Opportunities for students to develop positive attitudes and knowledge about present and future technologies in 3 or more of the following content areas:

*Areas in bold italics are emphasized content for grade 7 & 8 Technology Education.

*Areas in italics include exposed content the extent of instruction varies based on student interest and need.

a. Medical technologies;

b. Agricultural;

c. Biotechnologies;

d. ***Energy and power technologies***;

e. *Information and communications technologies*;

f. *Transportation technologies*;

g. ***Manufacturing technologies***;

h. ***Construction technologies***; and

i. *New and emerging technologies*;

(3) Opportunities for students to develop a knowledge and understanding of how social forces like demographics and prevailing economic systems can influence the free-enterprise system and the global marketplace;

"Supply and Demand" manufacturing unit for grade 8

(4) Opportunities to promote the development of problem-solving skills as well as basic skills in planning, design, fabrication, and evaluating technical processes technology/engineering principles and design, encouraging those habits of mind necessary to be a lifelong learner; and

Each hands-on project relies on the enhancement of these skills.

(5) Systematic instruction and activities designed to enable students to:

a. Acquire an understanding of technical processes, the practical application of mathematics and scientific principles, and the interrelationships between technology/engineering education and other academic disciplines in the school curriculum;

All build units rely on application of mathematics, engineering design process, and English Language Arts for communication.

b. Be aware of the right to, and the knowledge of what constitutes, safe work environments as well as the safe and appropriate use of tools, small machines, and processes;

Required prior to any machine exposure and use.

c. Understand industry and technology, their systematic structures, and their place in our culture;

"Supply and Demand" manufacturing unit for grade 8

d. Understand the technological systems model requiring inputs, processes, outputs and feedback, where the processes include the resources of people, information, tools, energy, capital, time, materials;

This is incorporated into material selection instruction.

e. Learn leadership and group-process skills;

All build units require students to work together and assume roles to facilitate group-process skills.

f. Recognize and build upon individual talents and interests; and

Units will offer student choice—not all students will create the same product or utilize the same materials.

g. Become familiar with opportunities and requirements for careers in new and emerging technologies like medicine, agriculture, biotechnology, energy and power, information and communications, transportation, manufacturing, and construction.

Collaborate with school counselor and utilize Naviance applications.

Source. #5546, eff 7-1-93; ss by #6366, eff 10-30-96, EXPIRED: 10-30-04

New. #8206, INTERIM, eff 11-18-04, EXPIRED: 5-17-05

New. #8354, eff 7-1-05; ss by #10556, eff 3-27-14; ss by #10870, EMERGENCY, eff 6-29-15,EXPIRED: 12-26-15; ss by #11020, eff 1-8-16 (See Revision Note at part heading for Ed 306)

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
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. https://www.education.nh.gov/career/career/documents/tech_ed_curr_guide.pdf

	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: *Why is this topic and skill set important for students? Consider the value of the content...*	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: *In 2-4 sentences, describe the desired results for students to have by the end of the unit.* *"Students will read/listen to ___ in order to ___"*	Students will design and build a bridge to span a certain distance that can withstand a given stress (different for each group). Students will listen to instruction relative to the			

"Students will show learning by using writing and/or speaking to ____"	safe operation of instrumentation and work together in a team with assigned team roles for the design, development, and modification of said device.			
Priority-Level Standards: *List only the standards which will be explicitly taught and assessed.*	A, B, C in tech ed curriculum guide			
Key Resources: *List 2-3 authentic and relevant resources that students will read and/or listen to. Include tests, videos, etc.*	• Equipment Safety Video • Safety Standards Assessment • Equipment Performance Assessment • Bridge assessment • Tools for design https://www.education.nh.gov/career/career/documents/tech_ed_curr_guide.pdf			

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
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. https://www.education.nh.gov/career/career/documents/tech_ed_curr_guide.pdf

	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: *Why is this topic and skill set important for students? Consider the value of the content...*	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: *In 2-4 sentences, describe the desired results for students to have by the end of the unit.* *"Students will read/listen to ___ in order to ___"* *"Students will show*	Students will design and build a device to amplify sound. Students will listen to instruction relative to the safe operation of instrumentation and work together in a team with assigned team roles for the			

learning by using writing and/or speaking to ____"	design, development, and modification of said device.			
Priority-Level Standards: *List only the standards which will be explicitly taught and assessed.*	A, B, C, D			
Key Resources: *List 2-3 authentic and relevant resources that students will read and/or listen to. Include tests, videos, etc.*	• Equipment Safety Video • Safety Standards Assessment • Equipment Performance Assessment • Sound amplification assessment • Tools for design https://www.education.nh.gov/career/career/documents/tech_ed_curr_guide.pdf			

Standards Matrix

	Goals (Standards) Technology/Engineering Education will contribute to the development of all students by:	**Unit 1**	**Unit 2**	**Unit 3**
Standard A	**Providing opportunities to develop safe and appropriate skills and awareness in a wide range of traditional and contemporary technologies.**	7, 8		
Standard B	**Providing opportunities to plan, develop, operate, control, and maintain a variety of technological systems such as medical, agricultural, biological, energy and power, information and communication, transportation, manufacturing, construction, and engineering.**	7, 8		
Standard C	**Preparing students to recognize, use and prepare technical information in order to engineer solutions to problems related to a variety of technological systems.**	7, 8		
Standard D	**Encouraging those habits of mind necessary to a lifelong learner such as the ability to question, investigate, design, experiment, and evaluate.**	8		
Standard E	**Promoting an appreciation for the interdependency of technology and other disciplines.**			

Standard F	**Increasing understanding of the relationships between technology, individuals, and society.**			
Standard G	**Providing an introduction to the impact technology has on society and the environment.**			
Standard H	**Encourage the development of leadership abilities through participation in extracurricular activities such as the Technology Student Association and projects that support their communities.**			

STATUS REPORT: SAU41 & SB1612

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

HB 1612 Signed by Governor Sununu June 18, 2018

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

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

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

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

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

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

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

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

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

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

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

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

SAU 41
HOLLISBROOKLINE

Prior to HB1612:

Data Security Framework was implemented

Assigned Roles

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

Updated the Acceptable Use Agreement (AUA)

- reviewed with new lens

Prepared a Software Inventory

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

SAU 41
HOLLISBROOKLINE

Per HB1612, inventoried, reviewed and vetted existing software applications

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

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

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

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

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

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

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

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

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

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

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

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

SAU 41
HOLLISBROOKLINE

Compiled and distributed an inventory of all district software

Unlicensed **Software**

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

Information must be submitted

Implemented Software Security Guidelines

Began with those submitted

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

Required Cloud-Based Technology Use Request Form

- Vetted individual submissions
- Set permissions based on need

SAU 41
HOLLISBROOKLINE

Developed Protocols for Protection of Student Data

Some resources require logins

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

How do we communicate our practices

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

SAU 41
HOLLISBROOKLINE

Conducted Mandatory Student Privacy and Data Security Trainings in June 2018

Training Included:

Cloud-Based Software Criteria

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

Guidelines for Data Privacy and Security

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

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

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

SAU 41
HOLLISBROOKLINE

SAU 41 Technology Initiative Approval Request

Cloud Based Software Services

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

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

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

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

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

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

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

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

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

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

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

Staff Member: _____ Date: _____

Principal: _____ Date: _____

For SAU Office Use Only

Approval Request Process:
Date Received_____ Initials _____

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

Signatures once approved/disapproved:
Business Administrator_____ Date: _____

Network Administrator _____ Date: _____

Assistant Superintendent _____ Date: _____

Student Data

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

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

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

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

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

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

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

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

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

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

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

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

SAU 41
HOLLISBROOKLINE

www.sau41.org

Search Site

SAU41 School Districts

Hollis and Brookline, New Hampshire

Administration | SAU 41 | Districts | Curriculum | Contacts | Resources | Quick Links

SAU41 Software List | Reports | How-To Guides | Technology Policies | Live Stream

Information Technology

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

Technology Use and Student Privacy

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

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

Helpful Links

- SAU 41 Software List
- SAU 41 AUA
- FERPA for Parents and Students (US DOE)
- Student Privacy 101 (US DOE)
- SAU 41 Technology Plan

SAU 41 Software List

SAU41 Software

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

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

* Approved with expressed parent permission

SAU 41 HOLLISBROOKLINE

Data Governance Plan

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Eighteen

AN ACT relative to data security in schools.

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

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

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.

Data Governance Plan Development

Data Governance Team

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

Define Data Lifecycle & Data Security

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

SAU 41
HOLLISBROOKLINE

Data Governance Plan

Plan for Critical Incident Response

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

Policy Work

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

SAU 41
HOLLISBROOKLINE

Next Steps

Tackling the Requirements

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

Ongoing Work…

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

SAU 41
HOLLISBROOKLINE

SAU41

Data Governance Plan

April, 2019

Contents

Introduction

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

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

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

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

Data Governance Team

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

Purpose

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

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

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

Scope

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

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

Regulatory Compliance

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

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

NH RSA 359-C:19 - Notice of Security Breach Definitions

NH RSA 359-C:20 - Notice of Security Breach Required

NH RSA 359-C:21 - Notice of Security Breach Violation

Data User Compliance

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

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

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

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

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

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

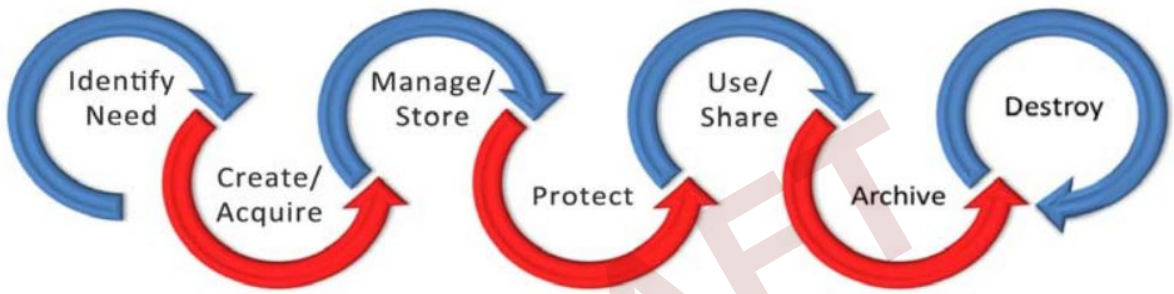
Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

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

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

Data Lifecycle

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



Identifying Need & Assessing Systems for District Requirements

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

New Systems

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

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

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

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

- Curricular value

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

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

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

Review of Existing Systems

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

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

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

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

Acquisition and Creation

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

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

Management and Storage

Systems Security

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

Data Management

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

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

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

accuracy and security of data.

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

Data Classification and Inventory

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

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

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

Security/Protection

Risk Management

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

Security Logs

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

Physical Security Controls

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

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

Inventory Management

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

Virus, Malware, Spyware, Phishing and SPAM Protection

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

Electronic Access Security Controls

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

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

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

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

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

Staff Users

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

to the ISOs with a clear justification for access.

Contractors/Vendors

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

Password Security

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

Concurrent Sessions

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

Remote Access

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

Securing Data at Rest and Transit

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

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

Usage and Dissemination

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

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

and Student Records (JRA, JRA-R).

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

Data Storage and Transmission

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

Cloud Storage and File Sharing

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

File Transmission Practices

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

Credit Card and Electronic Payment

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

Mass Data Transfers

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

Printing

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

Oral Communications

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

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

Training

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

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

Archival and Destruction

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

District Data Destruction Processes

The district will regularly review all existing data stored on district provided storage for the purposes of ensuring data identification and appropriate destruction. Data destruction processes will align with School Board Policy EHB and EHB-R. District data managers will regularly review systems and data to ensure that data that is no longer needed is destroyed. The following exceptions will be made:

- Data in an active litigation hold will be maintained until the conclusion of the hold.
- Student G Suite for Education account will be suspended after the final day of enrollment and maintained for one school year after the student's final date of attendance.
- Staff G Suite for Education accounts will be suspended after the final work day, unless HR or the ISOs approves a district administrator to maintain access.

Asset Disposal

The district will maintain a process for physical asset disposal in accordance with School Board Policy DN. The district will ensure that all assets containing PII, confidential, or internal information are disposed of in a manner that ensures that this information is destroyed (see Appendix H: Asset Management).

Critical Incident Response

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

Business Continuity

The District's administrative procedure EHB-R, delineates the timeline for data retention for all district data. The District will maintain systems that provide near-line and off-site data backup. These systems shall allow for the full recovery of critical systems in the event of a disaster. The district will test near-line and off-site backups of critical systems quarterly.

Disaster Recovery

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

Data Breach Response

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

Appendix A - Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix B - Laws, Statutory, and Regulatory Security Requirements

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

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

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

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

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

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

PPRA: The Protection of Pupil Rights Amendment affords parents and minor students' rights regarding our conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.
https://www2.ed.gov/policy//gen/guid/fpco/ppra/index.html

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

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

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

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

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

Appendix C - Digital Resource Acquisition and Use

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

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

New Resource Acquisition

Staff are required to complete steps outlined under the District's Staff Technology page on the SAU41 website. An online cloud/website tool request form is required for any new digital resources to be used in the classroom. All staff must adhere to the following guidelines regarding digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the Data Governance Team prior to initiation. Staff should speak with their building Technology Integrator before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be accessing content and/or any site that requires any student login.
- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the Data Governance Team.

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

- Impact on technology environment including storage and bandwidth
- Hardware requirements, including any additional hardware
- License requirements/structure, number of licenses needed, and renewal cost
- Maintenance agreements including cost
- Resource update and maintenance schedule
- Funding for the initial purchase and continued licenses and maintenance
- Terms of service, privacy policy, and MOU/contract that meet the following criteria:
    - o The district continues to own the data shared, and all data must be available to the district upon request.
    - o The vendor's access to and use of district data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.
    - o District data will be maintained in a secure manner by applying appropriate technical, B3 physical and administrative safeguards to protect the data.
    - o The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
    - o No API will be implemented without full consent of the district.
    - o All data will be treated in accordance to federal, state and local regulations

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

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

Approved Digital Resources

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

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

Digital Resource Licensing/Use

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

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

- Only approved district resources are to be used.
- District software licenses will be:
  - 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.

Appendix F - Securing Data at Rest and Transit

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

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

Cloud Storage and File Sharing

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

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

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

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

External Storage Devices

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

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

File Transmission Practices

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

Credit Card and Electronic Payment

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

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

• The district will never maintain a data system for payment information. All payment information will be stored and processed by a 3rd party accessible through a secure portal.

• Never request cardholder information to be transmitted via email or any other electronic communication system.

• Payment information shall be entered directly into the approved payment system by individual making payment. If the individual is not able to directly input the payment, designated staff may gain verbal approval for the payment process either in person or via phone (after identification is verified). If verbal payment information is received, that information must be entered directly into the payment system and not written down during the process.

Appendix G - Physical Security Controls RRTask

The following physical security controls shall be adhered to:

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

Appendix H - Asset Management

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

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

Inventory

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

Disposal Guidelines

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

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

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

Methods of Disposal

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

Discard

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

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

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

Donation/Gift

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

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

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

Internet Filtering

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

Phishing and SPAM Protection

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

Security Patches

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

Appendix J - Account Management

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

Staff Accounts

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

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

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

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

Local/Domain Administrator Access

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

Remote Access

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

Contractors/Vendors

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

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

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

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

Access accounts for the District's SIS are setup based on staff role/position, building and required access to student data and are assigned by the Database Manager. Teacher accounts are created for all staff responsible for taking student attendance and entering and maintaining grades. Teacher accounts login to the SIS Teacher Portal. Staff assigned a Teacher account only have access to students they teach or provide services. Administrative accounts are created based on the staff member's role/position and function and further restrictions to data are controlled through security groups. Security groups control access permissions to certain data sets such as attendance, demographic data, grades, discipline etc. and whether the staff member can view or maintain data. Additional page level permissions are assigned to the security groups. Administrative accounts log into the SIS Admin Portal.

SIS Security Groups*

- Administrator
- Athletic
- Counselor
- IT Staff
- Office Staff
- Principal
- Registrar
- Nurse
- Secretary II
- Super Amin
- Unassigned - no access

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

Financial System

All staff members are entered into the District's financial system for the purpose of staff payroll and HR tracking. Staff access to their individual payroll information is granted through the employee portal. Only staff requiring access are provided accounts for the financial/personnel system.

After basic information and user ID are created, a security role is assigned to the account granting them access to designated areas of the financial system to complete their job responsibilities.

Financial System Security Roles

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

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

Special Education System

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

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

Health Software System

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

Food Services System

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

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

Security Roles

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

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

Appendix L - Password Security

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

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

District network access to resources managed through LDAP

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

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

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

Appendix M - Technology Disaster Recovery Plan

Objectives

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

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

Planning Assumptions

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

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

Disaster Recovery/Critical Failure Team

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

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

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

Activation

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

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

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

Notification

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

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

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

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

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

Implementation

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

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

Deactivation

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

Evaluation

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

Appendix N - Data Breach Response Plan

Objectives

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

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

Planning Assumptions

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

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

Data Breach/Incident Response Team

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

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

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

Activation

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

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

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

Notification

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

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

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

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

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

Implementation

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

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

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

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

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

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

The following will take place during the incident response:

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

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

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

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

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

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

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

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

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

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

Deactivation

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

Evaluation

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

New Hampshire Department of Education

FY2020

GENERAL ASSURANCES, REQUIREMENTS AND DEFINITIONS FOR PARTICIPATION IN FEDERAL PROGRAMS

Subrecipients of any Federal grant funds provided through the New Hampshire Department of Education (NHDOE) must submit a signed copy of this document to the NHDOE Bureau of Federal Compliance prior to any grant application being deemed to be "substantially approvable". Once a grant is deemed to be in substantially approvable form, the subrecipient may begin to obligate funds which will be reimbursed upon final approval of the application by the NHDOE (34 CFR 708).

Any funds obligated by the subrecipient prior to the application being in substantially approvable form will not be reimbursable even upon final approval of the application by the NHDOE.

This FY2020 general assurances document contains some differences from the FY2019 general assurances document. You are encouraged to do a side by side comparison of the two documents so that you thoroughly understand the requirements to which you are agreeing.

Following your review and acceptance of these General Assurances, Requirements and Definitions for Participation in Federal Programs please sign the certification statement on the appropriate page and then initial each of the remaining pages where indicated.

Please note that the practice of the School Board authorizing the Superintendent to sign on behalf of the School Board Chair is not acceptable to the NHDOE in this case and will be considered non-responsive.

Once the document is fully executed, you may either email or mail a copy of the entire document to:

Timothy Carney
New Hampshire Department of Education
Bureau of Federal Compliance
101 Pleasant Street
Concord, NH 03301
Timothy.Carney@doe.nh.gov

Should you have any questions please contact Timothy Carney at 603-271-2634 or Lindsey Scribner at 603-271-3837.

General Assurances, Requirements and Definitions for Participation in Federal Programs

A. General Assurances

Assurance is hereby given by the subrecipient that, to the extent applicable:

1) The subrecipient has the legal authority to apply for the federal assistance, and the institutional, managerial, and financial capability (including funds sufficient to pay non-federal share of project costs, as applicable) to ensure proper planning, management, and completion of the project described in all applications submitted.

2) The subrecipient will give the awarding agency, the NHDOE, the Comptroller General of the United States and, if appropriate, other State Agencies, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award; and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.

3) The subrecipient will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.

4) The subrecipient will initiate and complete the work within the applicable time frame after receipt of approval of the awarding agency.

5) The subrecipient will comply with all Federal statutes relating to nondiscrimination. These include but are not limited to:
   (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin;
   (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C.§§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex;
   (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps;
   (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. §§6101-6107), which prohibits discrimination on the basis of age;
   (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse;
   (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism;
   (g) §§523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee-3), as amended, relating to confidentiality of alcohol and drug abuse patient records;
   (h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing;
   (i) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and,
   (j) the requirements of any other nondiscrimination statute(s) which may apply to the application.

6) The subrecipient will comply, or has already complied, with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of federal or federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of federal participation in purchases.

7) The subrecipient will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with federal funds. The subrecipient further assures that no federally appropriated funds have been paid or will be paid by or on behalf of the subrecipient to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the making of any federal grant; the entering into of any cooperative agreement; and the extension, continuation, renewal, amendment, or modification of any federal grant or cooperative agreement.

8) The subrecipient will comply with P.L. 93-348 regarding the protection of human subjects involved in research, development, and related activities supported in whole or in part with federal funds.

9) The subrecipient will comply with the Laboratory Animal Welfare Act of 1966 (P.L. 89-544, as amended, 7 U.S.C. §§2131 et seq.) pertaining to the care, handling, and treatment of warm blooded animals held for research, teaching, or other activities supported in whole or in part with federal funds.

10) The subrecipient will comply with the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. §§4801 et seq.) which prohibits the use of lead-based paint in construction or rehabilitation of residence structures.

11) The subrecipient will comply with all applicable requirements of all other federal laws, executive orders, regulations, and policies governing all program(s).

12) The subrecipient will cause to be performed the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and 2 CFR 200, Subpart F, "Audit Requirements," as applicable.

13) The recipient will comply with the requirements of Section 106(g) of the Trafficking Victims Protection Act (TVPA) of 2000, as amended (22 U.S.C. 7104) which prohibits grant award recipients or a sub-recipient from (1) Engaging in severe forms of trafficking in persons during the period of time that the award is in effect (2) Procuring a commercial sex act during the period of time that the award is in effect or (3) Using forced labor in the performance of the award or subawards under the award.

14) The control of funds provided to the subrecipient under each program, and title to property acquired with those funds, will be in a public agency, and a public agency will administer those funds and property.

15) Personnel funded from federal grants and their subcontractors will adhere to the prohibition from text messaging while driving an organization-owned vehicle, or while driving their own privately owned vehicle during official Grant business, or from using organization-supplied electronic equipment to text message or email while driving. Recipients must comply with these conditions under Executive Order 13513, "Federal Leadership On Reducing Text Messaging While Driving," October 1, 2009 (pursuant to provisions attached to federal grants funded by the US Department of Education).

16) The subrecipient assures that is will adhere to the Pro-Children Act of 2001, which states that no person shall permit smoking within any indoor facility owned or leased or contracted and utilized for the provision of routine or regular kindergarten, elementary, or secondary education or library services to children (P.L. 107-110, section 4303[a]). In addition, no person shall permit smoking within any indoor facility (or portion of such a facility) owned or leased or contracted and utilized for the provision of regular or routine health care or day care or early childhood development (Head Start) services (P.L. 107-110, Section 4303[b][1]). Any failure to comply with a prohibition in this Act shall be considered to be a violation of this Act and any person subject to such prohibition who commits such violation may be liable to the United States for a civil penalty, as determined by the Secretary of Education (P.L. 107-110, section 4303[e][1]).

17) The subrecipient will comply with the Stevens Amendment.

18) The subrecipient will submit such reports to the NHDOE and to U.S. governmental agencies as may reasonably be required to enable the NHDOE and U.S. governmental agencies to perform their duties. The recipient will maintain such fiscal and programmatic records, including those required under 20 U.S.C. 1234f, and will provide access to those records, as necessary, for those Departments/agencies to perform their duties.

19) The subrecipient will assure that all applications submitted for project/grant funding are proper and in accordance with the terms and conditions of the applications, the official who is authorized to legally bind the recipient agency/organization agrees to the following certification.

    "By signing this General Assurances, Requirements and Definitions for Participation in Federal Programs Document, I certify to the best of my knowledge and belief that all applications submitted are true, complete, and accurate, for the purposes and objectives set forth in the application, I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal or administrative penalties for false statements, false claims or otherwise."

20) The subrecipient will assure that expenditures reported are proper and in accordance with the terms and conditions of any project/grant funding, the official who is authorized to legally bind the agency/organization agrees to the following certification for all fiscal reports and/or vouchers requesting payment.

    "By signing this General Assurances, Requirements and Definitions for Participation in Federal Programs Document, I certify to the best of my knowledge and belief that the reports submitted are true, complete, and accurate, and the expenditures, disbursements and cash receipts are for the purpose and objectives set forth in the terms and conditions of the Project Award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise."

21) The subrecipient will provide reasonable opportunities for systematic consultation with and participation of teachers, parents, and other interested agencies, organizations, and individuals, including education-related community groups and non-profit organizations, in the planning for and operation of each program.

22) The subrecipient shall assure that any application, evaluation, periodic program plan, or report relating to each program will be made readily available to parents and other members of the general public upon request.

23) The subrecipient has adopted effective procedures for acquiring and disseminating to teachers and administrators participating in each program, significant information from educational research, demonstrations, and similar projects, and for adopting, where appropriate, promising educational practices developed through such projects. Such procedures shall ensure compliance with applicable federal laws and requirements.

24) The subrecipient will comply with the requirements of the Gun-Free Schools Act of 1994.

25) The subrecipient will submit a fully executed and accurate Single Audit Certification form to the NHDOE not later than March 31, 2020. The worksheet will be provided to each subrecipient by the NHDOE.

26) The subrecipient shall comply with the restrictions of New Hampshire RSA 15:5.

27) The subrecipient will comply with the requirements in 2 CFR Part 180, Government-wide Debarment and Suspension (Non-procurement).

28) The subrecipient certifies that it will maintain a drug-free workplace and will comply with the requirements of the Drug-Free Workplace Act of 1988.

29) The recipient will adhere to the requirements of Title 20 USC 7197 relative to the Transfer of Disciplinary Records.

B. Explanation of Grants Management Requirements

The following section elaborate on certain requirements included in legislation or regulations referred to in the "General Assurances" section. This section also explains the broad requirements that apply to federal program funds.

1. Financial Management Systems

Financial management systems, including records documenting compliance with federal statutes, regulations, and the terms and conditions of the federal award, must be sufficient to permit the preparation of reports required by general and program-specific terms and conditions; and the tracing of funds to a level of expenditures adequate to establish that such funds have been used according to the Federal statutes, regulations, and the terms and conditions of the Federal award.

Specifically, the financial management system must be able to:

a) Identify, in its accounts, all federal awards received and expended and the federal programs under which they were received. Federal program and federal award identification must include, as applicable, the CFDA title and number, federal award identification number and year, name of the federal agency, and name of the pass-through entity, if any.
b) Provide accurate, current, and complete disclosure of the financial results of each federal award or program.
c) Produce records that identify adequately the source and application of funds for federally funded activities.
d) Maintain effective control over, and accountability for, all funds, property, and other assets. The subrecipient must adequately safeguard all assets and assure that they are used solely for authorized purposes.

e) Generate comparisons of expenditures with budget amounts for each federal award.

2. Written Policies and Procedures

The subrecipient must have written policies and procedures for:

a) Cash Management (2 CFR 200.302(b)(6) & 200.305)
b) Determining the allowability of costs in accordance with 2 CFR 200 Subpart E—Cost Principles and the terms and conditions of the Federal award. (2 CFR 200.302(b)(7))
c) Conflict of Interest (2 CFR 200.318(c))
d) Procurement (2 CFR 200.320)
e) Method for conducting Technical Evaluations of Proposals and Selecting Recipients (2 CFR 200.320(d)(3) and 200.323)
f) Suspension and Debarment (2 CFR 200.213)
g) Travel Policy (2 CFR 200.474(b))
h) Equipment and Supplies (2 CFR 200.313(d), 200.314)
i) Time and Effort (2 CFR 200.430(i))
j) Record Keeping (2 CFR 200.333 and 200.335)

3. Internal Controls

The subrecipient must:

a) Establish and maintain effective internal control over the federal award that provides reasonable assurance that the non-federal entity is managing the federal award in compliance with federal statutes, regulations, and the terms and conditions of the federal award. These internal controls should be in compliance with the guidance outlined in "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States or the "Internal Control Integrated Framework", issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
b) Comply with federal statutes, regulations, and the terms and conditions of the federal awards.
c) Take prompt action when instances of noncompliance are identified, including noncompliance identified in audit findings.
d) Take reasonable measures to safeguard and protect personally identifiable information and other information the federal awarding agency or pass-through entity designates as sensitive or the subrecipient considers sensitive consistent with applicable federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.
e) Maintain all accounts, records, and other supporting documentation pertaining to all costs incurred and revenues or other applicable credits acquired under each approved project in accordance with 2 CFR 200.333.

4. Allowable Costs

In accounting for and expending project/grant funds, the subrecipient may only charge expenditures to the project award if they are;

a) in payment of obligations incurred during the approved project period;
b) in conformance with the approved project;
c) in compliance with all applicable statutes and regulatory provisions;
d) costs that are allocable to a particular cost objective;
e) spent only for reasonable and necessary costs of the program; and
f) not used for general expenses required to carry out other responsibilities of the subrecipient.

5. Audits

This part is applicable for all non-federal entities as defined in 2 CFR 200, Subpart F.

a) In the event that the subrecipient expends $750,000 or more in federal awards in its fiscal year, the subrecipient must have a single or program-specific audit conducted in accordance with the provisions of 2 CFR 200, Subpart F. In determining the federal awards expended in its fiscal year, the subrecipient shall consider all sources of federal awards, including federal resources received from the NHDOE. The determination of amounts of federal awards expended should be in accordance with the guidelines established by 2 CFR 200, Subpart F.
b) In connection with the audit requirements, the subrecipient shall also fulfill the requirements relative to auditee responsibilities as provided in 2 CFR 200.508.
c) If the subrecipient expends less than $750,000 in federal awards in its fiscal year, an audit conducted in accordance with the provisions of 2 CFR 200, Subpart F, is not required. In the event that the subrecipient expends less than $750,000 in federal awards in its fiscal year and elects to have an audit conducted in accordance with the provisions of 2 CFR 200, Subpart F, the cost of the audit must be paid from non-federal resources (i.e., the cost of such an audit must be paid from subrecipient resources obtained from non-federal entities).

The subrecipient assures it will implement the following audit responsibilities;

a) Procure or otherwise arrange for the audit required by this part in accordance with auditor selection regulations (2 CFR 200.509), and ensure it is properly performed and submitted nine months after the close of the fiscal year in accordance with report submission regulations (2 CFR 200.512).
b) Provide the auditor access to personnel, accounts, books, records, supporting documentation, and other information as needed so that the auditor may perform the audit required by this part.
c) Prepare appropriate financial statements, including the schedule of expenditures of federal awards in accordance with financial statements regulations (2 CFR 200.510).
d) Promptly follow up and take corrective action on audit findings, including preparation of a summary schedule of prior audit findings and a corrective action plan in accordance with audit findings follow-up regulations (2 CFR 200.511(b-c)).
e) Upon request by the NHDOE Bureau of Federal Compliance (BFC), promptly submit a corrective action plan using the NHDOE template provided by the BFC for audit findings related to NHDOE funded programs.
f) For repeat findings not resolved or only partially resolved, the subrecipient must provide explanation for findings not resolved or only partially resolved to the BFC for findings related to all NHDOE funded programs. The BFC will review the subrecipient's submission and issue an appropriate Management Decision in accordance with 2 CFR 200.521.

6. Reports to be Submitted

Audits/Management Decisions

Copies of reporting packages for audits conducted in accordance with 2 CFR 200, Subpart F shall be submitted, by or on behalf of the recipient directly to the following:

a) The Federal Audit Clearinghouse (FAC) in 2 CFR 200, Subpart F requires the auditee to electronically submit the data collection form described in 200.512(b) and the reporting package described in 200.512(c) to FAC at: https://harvester.census.gov/facides/(S(mqamohbpfj0hmyh1r45p1po1))/account/login.aspx

Copies of other reports or management decision letter(s) shall be submitted by or on behalf of the subrecipient directly to:

a) New Hampshire Department of Education
Bureau of Federal Compliance
101 Pleasant Street
Concord, NH 03301

b) In response to requests by a federal agency, auditees must submit a copy of any management letters issued by the auditor, 2 CFR 200.512(e).

Any other reports, management decision letters, or other information required to be submitted to the NHDOE pursuant to this agreement shall be submitted in a timely manner.

Single Audit Certification

An executed and accurate Single-Audit Certification form shall be submitted to the NHDOE not later than **March 31, 2020**. A copy of the form will be provided to each subrecipient by the NHDOE.

7. Debarment, Suspension, and Other Responsibility Matters

As required by Executive Orders (E.O.) 12549 and 12689, Debarment and Suspension, and implemented at 2 CFR Part 180, for prospective participants in primary covered transactions, as defined in 2 CFR 180.120, 180.125 and 180.200, no contract shall be made to parties identified on the General Services Administration's *Excluded Parties List System* as excluded from Federal Procurement or Non-procurement Programs in accordance with E.O.s 12549 and 12689, "Debarment and Suspension." This list contains the names of parties debarred, suspended, or otherwise excluded by agencies, and contractors declared ineligible under statutory or regulatory authority other than E.O. 12549. Contractors with awards that exceed the small purchase threshold shall provide the required certification regarding their exclusion status and that of their principal employees.

The federal government imposes this requirement in order to protect the public interest, and to ensure that only responsible organizations and individuals do business with the government and receive and spend government grant funds. Failure to adhere to these requirements may have serious consequences – for example, disallowance of cost, termination of project, or debarment.

To assure that this requirement is met, there are four options for obtaining satisfaction that subrecipients and contractors are not suspended, debarred, or disqualified. They are:

The subrecipient certifies that it and its principals:

a) Are not presently debarred, suspended, proposed for debarment, and declared ineligible or voluntarily excluded from covered transactions by any federal Department or agency.
b) Have not within a three-year period preceding this application been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction; violation of federal or state antitrust statutes; commission of embezzlement; theft, forgery, bribery, falsification, or destruction of records; making false statements; or receiving stolen property.
c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in this certification.

d) Have not within a three-year period preceding this application had one or more public transactions (federal, state, or local) terminated for cause or default.

Where the subrecipient is unable to certify to any of the statements in this certification, they shall attach an explanation to this document.

8. Drug-Free Workplace (Grantees Other Than Individual)

As required by the Drug-Free Workplace Act of 1988 and implemented in 34 CFR 84.200 and 84.610, the subrecipient certifies that it will continue to provide a drug-free workplace by:

a) Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the subrecipient's workplace and specifying the actions that will be taken against employees for violation of such prohibition.

b) Establishing, as required by 34 CFR 84.215, an ongoing drug-free awareness program to inform employees about:

   - The dangers of drug abuse in the workplace.
   - The recipient's policy of maintaining a drug-free workplace.
   - Any available drug counseling, rehabilitation, and employee assistance programs.
   - The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace.

c) Requiring that each employee engaged in the performance of the project is given a copy of this statement.

d) Notifying the employee in the statement that, as a condition of employment under the project, the employee will:

   - Abide by the terms of the statement.
   - Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction.

e) Notifying the agency in writing within 10 calendar days after receiving notice of an employee's conviction of a violation of a criminal drug statute in the workplace, as required by 34 CFR 84.205(c)(2), from an employee or otherwise receiving actual notice of employee's conviction. Employers of convicted employees must provide notice, including position title to:

   Director, Grants and Contracts Service
   U.S. Department of Education
   400 Maryland Avenue, S.W. [Room 3124, GSA – Regional Office Building No. 3]
   Washington, D.C. 20202-4571

(Notice shall include the identification number[s] of each affected grant).

f) Taking one of the following actions, as stated in 34 CFR 84.225(b), within 30 calendar days of receiving the required notice with respect to any employee who is convicted of a violation of a criminal drug statute in the workplace.

   - Taking appropriate personnel action against such an employee, up to and including

termination consistent with the requirements of the Rehabilitation Act of 1973, as amended.

- Requiring such employee to participate satisfactorily in drug abuse assistance or rehabilitation program approved for such purposes by a federal, state, or local health, law enforcement, or other appropriate agency.

g) Making a good-faith effort to maintain a drug-free workplace through implementation of the requirements stated above.

9. EDGAR - Education Department General Administrative Regulations

The federal grant administrative regulations for education (Title 34 CFR Parts 75, 76, 77, 79, 81, 82, 84, 86, 97, 98, and 99), was revised on December 26, 2014, with the implementation of the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Grants Guidance), and delete 34 CFR Parts 74, 80, and 85 (Part 85 changed to 2 CFR Part 180) and included the deleted regulations into the Uniform Grants Guidance. Both administrative regulations (EDGAR and Uniform Grants Guidance), apply to all federal projects/awards.

10. General Education Provisions Act (GEPA) Requirements - Section 427 (Federal Requirement) Equity for Students, Teachers, and Other Program Beneficiaries

The purpose of Section 427 of GEPA is to ensure equal access to education and to promote educational excellence by ensuring equal opportunities to participate for all eligible students, teachers, and other program beneficiaries in proposed projects, and to promote the ability of such students, teachers, and beneficiaries to meet high standards. Further, when designing their projects, grant applicants must address the special needs and equity concerns that might affect the ability of students, teachers, and other program beneficiaries to participate fully in the proposed project.

Program staff within the NHDOE must ensure that information required by Section 427 of GEPA is included in each application that the Department funds. *(There may be a few cases, such as research grants, in which Section 427 may not be applicable because the projects do not have individual project beneficiaries. Contact the Government Printing Office staff should you believe a situation of this kind exists).*

The statute highlights **six types of barriers that can impede equitable access or participation: gender, race, national origin, color, disability, and age**. Based on local circumstances, the applicant can determine whether these or other barriers may prevent participants from access and participation in the federally assisted project, and how the applicant would overcome these barriers.

These descriptions may be provided in a single narrative or, if appropriate, may be described in connection with other related topics in the application. Subrecipients should be asked to state in the table of contents where this requirement is met.

NHDOE program staff members are responsible for screening each application to ensure that the requirements of this section are met before making an award. If this condition is not met, after the application has been selected for funding the program staff should contact the subrecipient to find out why this information is missing. Documentation must be in the project file indicating that this review was completed before the award was made. If an oversight occurred, the program staff may give the applicant another opportunity to satisfy this requirement, but must receive the missing information before making the award, 34 CFR 75.231.

All applicants for new awards must satisfy this provision to receive funding. Those seeking *continuation* awards do not need to submit information beyond the descriptions included in their original applications.

11. Gun Possession (Local Education Agencies (LEAs) only)

As required by Title XIV, Part F, and Section 14601 (Gun-Free Schools Act of 1994) of the Improving America's Schools Act:

The LEA assures that it shall comply with the provisions of RSA 193:13 III.

> RSA 193:13, III. Any pupil who brings or possesses a firearm as defined in section 921 of Title 18 of the United States Code in a safe school zone as defined in RSA 193-D:1 without written authorization from the Superintendent or designee shall be expelled from school by the local school board for a period of not less than 12 months.

The LEA assures that it has adopted a policy, which allows the Superintendent or Chief Administrating officer to modify the expulsion requirement on a case by case basis. RSA 193:13, IV.

The LEA assures that it shall report to the NHDOE in July of each year, a description of the circumstances surrounding any expulsions imposed under RSA 193:13, III and IV including, but not limited to:

a) The name of the school concerned;
b) The grade of the student disciplined;
c) The type of firearm involved;
d) Whether or not the expulsion was modified, and
e) If the student was identified as Educationally Disabled.

The LEA assures that it has in effect a policy requiring referral to the criminal justice or juvenile delinquency system of any student who brings a firearm or weapon to school.

Ed 317.03 Standard for Expulsion by Local School Board.

a) A school board which expels a pupil under RSA 193:13, II or III, shall state in writing its reasons, including the act leading to expulsion, and shall provide a procedure for review as allowed under RSA 193:13, II.
b) School boards shall make certain that the pupil has received notice of the requirements of RSA 193-D and RSA 193:13 through announced, posted, or printed school rules.
c) If a student is subject to expulsion and a firearm is involved, the Superintendent shall contact local law enforcement officials whenever there is any doubt concerning:
    1) Whether a firearm is legally licensed under RSA 159; or
    2) Whether the firearm is lawfully possessed, as opposed to unlawfully possessed, under the legal definitions of RSA 159.
d) If a pupil brings or possesses a firearm in a safe school zone without written authorization from the Superintendent, the following shall apply:
    1) The Superintendent shall suspend the pupil for a period not to exceed 10 days, pending a hearing by the local board; and
    2) The school board shall hold a hearing within 10 days to determine whether the student was in violation of RSA 103:13, III and therefore is subject to expulsion.

12. Lobbying

As required by Section 1352, Title 31, of the U.S. Code, and implemented in 34 CFR Part 82, for persons entering into a grant or cooperative agreement over $100,000, as defined in 34 CFR 82.105 and 82.110,

the applicant certifies that:

a) No federally appropriated funds have been paid or will be paid by or on behalf of the subrecipient to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the making of any federal grant; the entering into of any cooperative agreement; and the extension, continuation, renewal, amendment, or modification of any federal grant or cooperative agreement.

b) If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with federal grants or cooperative agreements, the subrecipient shall complete and submit Standard Form - LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

c) The subrecipient shall require that the language of this certification be included in the award documents for all sub-awards at all tiers (including subcontracts, sub-grants, contracts under grants, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly.

New Hampshire RSA 15:5 - **Prohibited Activities.**

I. Except as provided in paragraph II, no recipient of a grant or appropriation of state funds may use the state funds to lobby or attempt to influence legislation, participate in political activity, or contribute funds to any entity engaged in these activities.

II. Any recipient of a grant or appropriation of state funds that wishes to engage in any of the activities prohibited in paragraph I, or contribute funds to any entity engaged in these activities, shall segregate the state funds in such a manner that such funds are physically and financially separate from any non-state funds that may be used for any of these purposes. Mere bookkeeping separation of the state funds from other moneys shall not be sufficient.

13. Subrecipient Monitoring

In addition to reviews of audits conducted in accordance with 2 CFR 200, Subpart F, subrecipient[ient monitoring procedures may include, but not be limited to, on-site visits by NHDOE staff, limited scope audits, and/or other procedures. By signing this document, the subrecipient agrees to comply and cooperate with any monitoring procedures/processes deemed appropriate by the NHDOE. In the event the NHDOE determines that a limited scope audit of the project recipient is appropriate, the subrecipient agrees to comply with any additional instructions provided by NHDOE staff to the subrecipient regarding such audit.

14. More Restrictive Conditions

Subrecipients found to be in noncompliance with program and/or fund source requirements or determined to be "high risk" shall be subject to the imposition of more restrictive conditions as determined by the NHDOE.

15. Obligations by Subrecipients

Obligations will be considered to have been incurred by subrecipients on the basis of documentary evidence of binding commitments for the acquisition of goods or property or for the performance of work, except that funds for personal services, for services performed by public utilities, for travel, and for the rental of facilities shall be considered to have been obligated at the time such services were rendered, such travel was performed, and/or when facilities are used (see 34 CFR 76.707).

16. Participation of Private School Students and Staff in Federal Grants

Students and staff of nonpublic schools shall be given an opportunity for equitable participation in activities or services conducted by school districts using federal funds. Appropriate personnel must be aware of, and consult, program-specific guidelines discussed in the applicable program statute, regulations, and guidance documents.

17. Personnel Costs – Time Distribution

Charges to federal projects for personnel costs, whether treated as direct or indirect costs, are allowable to the extent that they satisfy the specific requirements of 2 CFR 200.430, and will be based on payrolls documented in accordance with generally accepted practices of the subrecipient and approved by a responsible official(s) of the subrecipient.

When employees work solely on a single federal award or cost objective, charges for their salaries and wages must be supported by personnel activity reports (PARs), which are periodic certifications (at least semi-annually) that the employees worked solely on that program for the period covered by the certification. These certifications must be signed by the employee or a supervisory official having firsthand knowledge of the work performed by the employee.

When employees work on multiple activities or cost objectives (e.g., more than one federal project, a federal project and a non-federal project, an indirect cost activity and a direct cost activity, two or more indirect activities which are allocated using different allocation bases, or an unallowable activity and a direct or indirect cost activity), the distribution of their salaries or wages will be supported by personnel activity reports or equivalent documents that meet the following standards:

a) Reflect an after-the-fact distribution of the actual activity of each employee
b) Account for the total activity for which each employee is compensated
c) Prepared at least monthly and must coincide with one or more pay period
d) Signed and dated by the employee

18. Project Effective Dates

For federal programs, funds shall be obligated no earlier than the date the project application was received by the NHDOE and determined to be in substantially approvable form or the effective date of the federal grant award, whichever is later.

All Project/Grant Award Notifications reflect the beginning and ending dates of the project period and the date for submission of the final expenditure report. All conditions stated in the award notification are considered binding on the subrecipient.

19. Protected Prayer in Public Elementary and Secondary Schools

As required in Section 9524 of the Elementary and Secondary Education Act (ESEA) of 1965, as amended by the No Child Left Behind Act of 2001, LEAs must certify annually that they have no policy that prevents or otherwise denies participation in constitutionally protected prayer in public elementary

and secondary schools.

20. Purchasing

All subrecipients must have documented procurement policies and procedures that meet the minimum requirements of federal and state statutes, rules, and regulations. Under the Uniform Administrative Requirements, the procurement standards are located at 2 CFR 200.317 – 200.326.

22. Retention and Access to Records

Requirements related to retention and access to project/grant records, are determined by federal rules and regulations. Federal regulation 2 CFR 200.333, addresses the retention requirements for records that applies to all financial and programmatic records, supporting documents, statistical records, and all other non-Federal entity records pertinent to a Federal or Project award. If any litigation, claim, or audit is started before the expiration date of the retention period, the records must be maintained until all ligation, claims, or audit findings involving the records have been resolved and final action taken.

Access to records of the subrecipient and the expiration of the right of access is found at 2 CFR 200.336 (a) and (c), which states:

> a) Records of non-Federal entities. The Federal awarding agency, Inspectors General, the Comptroller General of the United States, and the pass-through entity, or any of their authorized representatives [including but not limited to the NHDOE] must have the right of access to any documents, papers, or other records of non-Federal entity which are pertinent to the Federal award, in order to make audits, examinations, excerpts, and transcripts. The right also includes timely and reasonable access to the non-Federal entity's personnel for the purpose of interview and discussion related to such documents.
>
> c) Expiration of right of access. The rights of access in this section are not limited to the required retention period but last as long as the records are retained.

23. The Stevens Amendment

All federally funded projects must comply with the Stevens Amendment of the Department of Defense Appropriation Act, found in Section 8136, which provides:

> *When issuing statements, press releases, requests for proposals, bid solicitations, and other documents describing projects or programs funded in whole or in part with federal money, all grantees receiving federal funds, including but not limited to state and local governments, shall clearly state (1) the percentage of the total cost of the program or project which will be financed with federal money, (2) the dollar amount of federal funds for the project or program, and (3) the percentage and dollar amount of the total costs of the project or program that will be funded by non-governmental sources.*

24. Transfer of Disciplinary Records

Title 20 USC 7197 requires that the State have a procedure to assure that a student's disciplinary records, with respect to suspensions and expulsions, are transferred by the project recipient to any public or private elementary or secondary school where the student is required or chooses to enroll. In New Hampshire, that assurance is statutory and found at RSA 193-D:8.

The relevant portions of the federal and state law appear below.

a) **Disciplinary Records -** In accordance with the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. 1232g), not later than 2 years after the date of enactment of this part, each State receiving Federal funds under this Act shall provide an assurance to the Secretary that the State has a procedure in place to facilitate the transfer of disciplinary records, with respect to a suspension or expulsion, by local educational agencies to any private or public elementary school or secondary school for any student who is enrolled or seeks, intends, or is instructed to enroll, on a full- or part-time basis, in the school.

b) **193-D:8 Transfer Records; Notice –** All elementary and secondary educational institutions, including academies, private schools, and public schools, shall upon request of the parent, pupil, or former pupil, furnish a complete school record for the pupil transferring into a new school system. Such record shall include, but not be limited to, records relating to any incidents involving suspension or expulsion, or delinquent or criminal acts, or any incident reports in which the pupil was charged with any act of theft, destruction, or violence in a safe school zone.

B. Definitions

1) **Audit finding** - A*udit finding* means deficiencies which the auditor is required by 2 CFR 200.516 Audit findings, paragraph (a) to report in the schedule of findings and questioned costs (2 CFR 200.5).

2) **Management decision** -*Management decision* means the evaluation by the Federal awarding agency or pass-through entity of the audit findings and corrective action plan and the issuance of a written decision to the auditee as to what corrective action is necessary (2 CFR 200.66).

3) **Obligations** - When used in connection with a non-Federal entity's utilization of funds under a Federal award, *obligations* means orders placed for property and services, contracts and subawards made, and similar transactions during a given period that require payment by the non-Federal entity during the same or a future period (2 CFR 200.71).

4) **Pass-through entity** - *Pass-through entity* means a non-Federal entity that provides a subaward to a subrecipient to carry out part of a Federal program (2 CFR 200.74).

5) **Period of performance** - *Period of performance* means the time during which the non-Federal entity may incur new obligations to carry out the work authorized under the Federal award. The Federal awarding agency or pass-through entity must include start and end dates of the period of performance in the Federal award.

6) **Subaward** - *Subaward* means an award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract. (2 CFR 200.92).

7) **Subrecipient -** *Subrecipient* means a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency (2 CFR 200.93).

CERTIFICATION

Instructions: The Superintendent, or other Qualifying Administrator, if the School District does not have a Superintendent, (*See* RSA 194-C:5, II) **must** consult with the School Board for the School District by informing said School Board about the District's participation in Federal Programs and the terms and conditions of the General Assurances, Requirements and Definitions for Participation in Federal Programs. The Superintendent or other Qualifying Administrator and the Chair of the School Board **must** sign this certification page (and initial the remaining pages) as described below and return it to the NHDOE. **No payment for project/grant awards will be made by the NHDOE without a fully executed copy of this General Assurances, Requirements and Definitions for Participation in Federal Programs on file.** For further information, contact the NHDOE Bureau of Federal Compliance at (603) 271-2634.

Superintendent or other Qualifying Administrator Certification:

We the undersigned acknowledge that [a] person is guilty of a violation of R.S.A. § 641:3 if [h]e or she makes a written or electronic false statement which he or she does not believe to be true, on or pursuant to a form bearing a notification authorized by law to the effect that false statements made therein are punishable; or (b) With a purpose to deceive a public servant in the performance of his or her official function, he or she: (1) Makes any written or electronic false statement which he or she does not believe to be true; or (2) Knowingly creates a false impression in a written application for any pecuniary or other benefit by omitting information necessary to prevent statements therein from being misleading; or (3) Submits or invites reliance on any writing which he or she knows to be lacking in authenticity; or (4) Submits or invites reliance on any sample, specimen, map, boundary mark, or other object which he or she knows to be false.

Accordingly, I, the undersigned official legally authorized to bind the named School District hereby apply for participation in federally funded education programs on behalf of the School District named below. I certify, to the best of my knowledge, that the below School District will adhere to and comply with these General Assurances, Requirements and Definitions for Participation in Federal Programs (pages 1 through 16 inclusive). I further certify, as is evidenced by the Minutes of the School Board/School Administrative Unit Meeting of _____ __, ____, that I have informed all members of the School Board of the federal funds the District will be receiving and of these General Assurances, Requirements and Definitions for the District's participation in said programs.

SAU Number: _____ School District:_____

_____	_____	_____
Typed Name of Superintendent Or other Qualifying Administrator	Signature	Date

Initials of Superintendent: _____
Initials of School Board Chair:_____

School Board Certification:

I, the undersigned official representing the School Board, acknowledge that the Superintendent, or other Qualifying Administrator, as identified above, has consulted with all members of the School Board, in furtherance of the School Board's obligations, including those enumerated in RSA 189:1-a, and pursuant to the School Board's oversight of federal funds the District will be receiving and of the General Assurances, Requirements and Definitions for Participation in Federal in said programs.

_____	_____	_____
Typed Name of School Board Chair (on behalf of the School Board)	Signature	Date

Please email or mail a copy of the entire document to:

Timothy Carney
New Hampshire Department of Education
Bureau of Federal Compliance
101 Pleasant Street
Concord, NH 03301

Timothy.Carney@doe.nh.gov

Initials of Superintendent: _____
Initials of School Board Chair:_____

LEA's. Individual program policy establishes which of these two entities may apply for federal funds. As such, both the Superintendent and the local School Board Chairperson are required to sign the certifications of the attached document.

I am requesting that you and the local School Board complete the certifications at the end of the enclosed general assurance document; initial each page in the spaces provided and return it in full to the attention of the Bureau of Federal Compliance. That office will notify the directors of all NHDOE programs approving federal funds to LEA's when they have received your assurances. The directors of the various federal programs are not to request additional copies from you, but to accept the Bureau of Federal Compliance list as the basis for determining compliance with these requirements as one item in their approval of proposals for funding. Other program specific assurances will still be requested from the LEA's by individual NHDOE programs.

Compliance with these general assurances will be subject to review by NHDOE staff during on-site federal compliance monitoring. Annual audits by CPA's in accordance with the Single Audit Act may also include compliance checks.

On the Certification page, please include the name and number of the SAU office and the name of the School District which will be applying for funds, both certifying parties are asked to execute the document, and return to the NHDOE Bureau of Federal Compliance office no later than **June 30, 2019**.

Thank you for your assistance with this initiative. This process should make it less difficult for all of us to access and use the federal funds for the purposes designated.

If you should have any questions regarding these general assurances, please contact Timothy Carney, Administrator of the Bureau of Federal Compliance at Timothy.Carney@doe.nh.gov or at 603-271-2634.

Enclosure

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.

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'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.

ILD

EDUCATIONAL QUESTIONNAIRES, SURVEYS AND RESEARCH

Protection of Pupil Rights Amendment

Pursuant to the Protection of Pupil Rights Amendment, no student will be required to submit to a survey, analysis, or evaluation which is administered or distributed by a school, and is funded in whole or in part by any program administered by the U.S. Department of Education without the prior written consent of the parent/guardian. ~~that reveals information concerning the following:~~ **Under RSA 186:11, IX-d, prior notice and prior consent (opt-in) is required for any non-academic survey designed to elicit information about:**

1. Political affiliations;

2. Mental and psychological problems potentially embarrassing to the student or the family;

3. Sexual behavior and attitudes;

4. Illegal, anti-social, self-incriminating, and demeaning behavior;

5. Critical appraisals of other individuals with whom respondents have close family relationships;

6. Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;

7. Religious practices, affiliations, or beliefs of the student or student's parent; or

8. Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

School District Approval

Any survey created by a third party or funded, in whole or in part, by the U.S. Department of Education, that includes any of the eight categories listed above, will be available for inspection by parents/guardians before the survey is administered to students. ~~Parents/guardians will have the right to deny permission for their child to participate in taking the survey. The school will not penalize students whose parents/guardians exercise this option.~~ The school will take reasonable precautions to protect student privacy during their participation of any survey, analysis, or evaluation containing one or more of the eight categories listed above. ***The school will not penalize any student whose parents or guardians choose not to opt in to surveys.***

Consent Exception for Youth Risk Behavior Survey Developed by the Centers for Disease Control and Prevention.

Neither state nor federal law requires prior written consent for administration of the Youth Risk Behavior Survey developed by the Centers for Disease Control and Prevention. Guidance issued by the Center for Disease Control, United States Department of Health and Human Services, concludes that federal law, including the Protection of Pupil Rights Amendment, also does not require prior written consent from parents or guardians because students are not required to participate and the survey is not paid for by the United States Department of Education.

However, New Hampshire law nonetheless requires the District to provide parents/guardians with notice at least ten (10) days before the Youth Risk Behavior Survey is administered. Parents may inspect the Youth Risk Behavior Survey at the school's administrative office. Parents or guardians may opt their student out of participating in the Youth Risk Behavior Survey by providing the Principal with written notice. District staff administering the Youth Risk Behavior Survey shall insure students understand that participation is voluntary and that students who opt-out will not be penalized.

Parental Notification

Parents will be notified when the school intends on issuing an educational survey. Notice will be given as early as possible before the survey is administered. Included in the notice will be information regarding how the survey or questionnaire will be administered; how it will be utilized; and the persons or entities that will have access to the results of the completed survey or questionnaire. Parents or guardians wishing to inspect a survey, analysis, or evaluation will be able to do so in the administrative office. Parents may refuse to allow their student to participate before or after reviewing the survey or questionnaire.

School District Use of Data

Administrators, teachers, other staff members and the school board may use surveys for many purposes. Such purposes may include, but are not limited to, the need for student services, the determination of prevailing views pertaining to proposed policies and/or practices, or the determination of student knowledge and/or attitudes related to a specific subject. These are examples of surveys and not intended to be an all-inclusive listing. Administrative approval is required for surveys. Responses will not be used in any identifying manner.
Surveys conducted for other agencies, organizations or individuals must have the recommendation of the Superintendent and the approval of the school board as to content and purpose. The results of such approved surveys must be shared with the school board.

Legal References:

20 U.S.C. § 1232h; 34 CFR Part 98, Protection of Pupil Rights Amendment

Appendix ILD-R

First Reading: May 15, 2013

Second Reading: June 19, 2013

Approved: July 17, 2013

Amendments:

First Reading: April 10, 2019

Second Reading: May 15, 2019

ADC

TOBACCO PRODUCTS BAN

(USE AND POSSESSION IN AND ON SCHOOL FACILITIES AND GROUNDS)

USE OF TOBACCO PRODUCTS STRICTLY PROHIBITED IN/ON ALL SCHOOL FACILITIES AND/OR GROUNDS

No person shall use any tobacco product in any facility maintained by the School District, nor on any of the grounds of the District.

"Tobacco products" means cigarettes, cigars, snuff, smokeless tobacco, smokeless cigarettes, chewing tobacco, E cigarettes, vaporizers, liquid nicotine, related liquid non-nicotine products and products containing tobacco, and tobacco in any other form.

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

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

It is the responsibility of the building principal(s), or designee, to initially enforce this policy by requesting that any person who is violating this policy to immediately cease the use of tobacco products. After this request is made, if any person refuses to refrain from using tobacco products in violation of this policy, the principal or designee may call the local police who shall then be responsible for all enforcement proceedings and applicable fines and penalties.

Students

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

Enforcement of this prohibition shall initially rest with building principals, or their designees, who may report any violation to the local police department. In accordance with state law, the police department shall be responsible for all proceedings and applicable fines and penalties.

The principal will develop regulations which cover disciplinary action to be taken for violations of this policy. These regulations will be communicated to students by means deemed

appropriate by the principal. In addition to disciplinary actions taken by the school, criminal penalties for fines may result from violations of this policy.

Employees

No employee shall use any tobacco product in any facility in any school vehicle or anywhere on school grounds maintained by the District.

Initial responsibility for enforcement of this prohibition shall rest with building principals, or their designees. The principal may report violations to the local police department. In accordance with state law, the police department shall be responsible for all proceedings and applicable fines and penalties.

The principal will develop and implement the appropriate means of notifying employees of the possible disciplinary consequences of violating this policy. Any employee(s) who violate(s) this policy is subject to disciplinary action which may include warning, suspension or dismissal. In addition, fines or other penalties may result from enforcement of these prohibitions by other law enforcement officials.

All other persons

No visitor shall at any time use tobacco products in any facility, in any school vehicle, or anywhere on school grounds maintained by the District.

Responsibility for enforcement of this prohibition shall rest with all School District employees who may report violations to the local police department. In accordance with state law, the police department shall be responsible for all proceedings and applicable fines and penalties.

Legal References:

RSA 155: 64 - 77, Indoor Smoking Act

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

RSA 126 - K:7, Use of Tobacco Products on Public Educational Grounds Prohibited

Adopted: May 24, 2004

First Reading: April 10, 2019 (as amended)

Second Reading: May 15, 2019 (as amended)

AC

NON-DISCRIMINATION

POLICY: The Hollis-Brookline Cooperative School District shall not discriminate in its education programs, activities, or employment practices on the basis of gender, sexual orientation, gender identity, race, color, religion, nationality, ethnic origin, age, marital status, or disability under the provisions of Title VI of the Civil Rights Act of 1964, Age Discrimination Act of 1967, and Title IX of the Education Amendment of 1972, and Section 504 of the Rehabilitation Act of 1973. Any person having inquiries concerning the District's compliance with the regulations implementing these laws may contact the Superintendent of Schools.

The District will not discriminate against an employee who is the victim of domestic violence, harassment, sexual assault, or stalking.

PROCEDURE~~:~~

The Superintendent or his/her designee will receive all inquiries, complaints, and other communications relative to this policy and the applicable laws and regulations concerned with non-discrimination. The Coordinator for Title IX is the building Principal or a designee as determined by the Superintendent of Schools.

Inquiries may be directed to the coordinators listed herein or to the Regional Office for Civil Rights, US Dept. of HHS, Government Center, JFK Federal Building, Room 1875, Boston, MA 02203 or the NH Human Rights Commission, 2 Chennel Drive, Concord, NH 03301 or the Special Education Bureau, NH Department of Education, 101 Pleasant Street, Concord, NH 03301.

Grievance procedures are available which provide for the prompt and equitable resolution of complaints alleging violations to Titles VI and IX, Section 504, and the Individuals with Disabilities Education Act of 1990. Grievance procedures may be obtained at the office of the Coordinators listed herein.

Legal Reference:

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

RSA 354-A:7, Unlawful Discriminatory Practices

The Age Discrimination in Employment Act of 1967

Title II of The Americans with Disabilities Act of 1990

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

RSA 186:11, XXXIII, Discrimination

RSA 275:71, Prohibited Conduct by Employer

ED 306

Adoption: November 17, 2004

First Reading: April 10, 2019 (as amended)

Second Reading: May 15, 2019 (as amended)

IJOC

See also GBCD

VOLUNTEERS

The Hollis Brookline Cooperative School Board recognizes the valuable contribution made to the total school program through the volunteer assistance of parents and other citizens. In working with volunteers, a District staff member shall clearly explain the volunteer's responsibility.

The Superintendent is responsible for developing and implementing procedures in accordance with RSA 189:13-a for the utilization of volunteers. The selection of volunteers will be consistent with those policies and procedures under the direction of the Superintendent. It is the responsibility of school administration to ensure that all volunteers are approved prior to allowing services to be rendered.

Designated Volunteers

Designated volunteers are subject to the provisions of Policy GBCD – Background Investigation and Criminal Records Check and will be required to undergo a background investigation and a criminal records check. "Designated volunteer" means any volunteer who:

1. Comes in direct contact with students;

2. Chaperones field trips, dances, athletics or activities as defined by the Superintendent;

3. Meets with students on a one-on-one basis;

4. Any other volunteer so designated by the School Board or Superintendent.

Supervised Volunteers

1. Are never left alone in the building;
2. Do not have regular, direct contact with children;
3. May not perform duties of designated volunteers.

Volunteer Requirements

A. Complete an application.
B. Complete annual training as defined by the Superintendent.
C. Serve in the capacity of assistants and not be assigned to roles which require specific professional training. Instructional services shall be rendered under the supervision of certified staff.
D. Sign a confidentiality agreement, and refrain from discussing the performance or actions of a student except with the student's teacher, counselor or Principal.
E. Refer any student problem that arises, whether of an instructional, medical or operational nature, to a regular staff member.

F. Receive orientation, including (1) general job responsibilities; (2) information about school facilities, routines, and procedures, including safety and evaluation; (3) expected relationship to regular staff.
G. Receive appropriate training at the building level, consistent with their tasks and existing District standards. This training shall be developed under the leadership of the Principal in consultation with the volunteer coordinator.
H. The school district employee with whom the volunteer is working should have assignments and activities clearly defined and in writing.
I. Volunteers may be terminated when:
    1. Program and/or duties are no longer needed;
    2. They are replaced by paid staff; or
    3. In the sole judgment of the administration; their conduct does not meet the standards of the District.
    4. The Superintendent reserves the right to sever the volunteer relationship at any time with or without cause.
J. Adhere to all district policies and procedures.

The voluntary help of citizens should be requested by staff through administrative channels to assist in conducting selected activities and/or to serve as resource persons. Staff members shall receive training in assignment of duties, supervision, and evaluation of volunteers.

Volunteer coaches of individual sports must be certified in that sport and be in compliance with the standards set by NHIAA., Tri-County or as defined by SAU 41 Administration. (http://66.223.48.174/PDFs/515/Memo_Explaining_Interim.pdf)

Volunteers should only function under direct supervision of a school employee. Employees of SAU 41 and its member districts wishing to volunteer in any capacity are subject to the same requirements as non-employee volunteers.

Legal Reference:

RSA 189:13-a, School Employee Volunteer Background Investigations

1st Reading: September 21, 2005
Adopted: May 21, 2008
Amended: February 18, 2009
1st Reading: April 10, 2019
2nd Reading: May 15, 2019