SCHOOL ADMINISTRATIVE UNIT THIRTY-NINE
Amherst, Mont Vernon, and Souhegan Cooperative School Districts

ADAM A. STEEL
Superintendent of Schools

CHRISTINE M. LANDWEHRLE
Assistant Superintendent

MARGARET A BEAUCHAMP
Director of Student Services

SAU #39 Board Meeting Agenda

Thursday, May 23, 2019 – 6:00 PM
Brick School
1 School Street
Amherst, NH 03031

Agenda Item	Time	Desired Action	Backup Materials
Call to Order	*6:00 PM*		None
Public Input I of II	*6:05 PM*		None
Board Updates	*6:10 PM*	No Action Needed *Each School Board to give an update on their Districts- ASD, MVSD, SCSD*	None
PD Committee Rep.	*6:15PM*	*Board to select a PD Committee Representative.*	None
Superintendent's Report	*6:20 PM*	*Mr. Steel to present his Superintendent's Report*	None
Consent Agenda-Approval	*6:30 PM*	1. Draft Minutes of April 16, 2019 2. 2019-03 SAU39 Treasurer's Report 3. Deputy Treasurer Appointment 4. Policies- Second Reading from 4/16 Meeting- DA, DB, DBB, DBC, DC, DD, DEA, DFA, DG, DGA, DH, DI, DIA, DIAM, DID, EHAA, EHAB, and ADB/ GBEC	Draft Minutes 04 16 2019 Treasurer Report Mar. 2019 None Policy Packet
First Read Policies- For SAU and motion to move to individual Boards	*6:35PM*	*Board to discuss policies for a first reading for SAU and motion to move to individual Boards- DBF, DBI, DBJ, EHB, EHB-R, and KE/KEB*	Policy Packet
Audit RFP	*6:40 PM*	*Action needed for the Board to select an Auditor.*	Audit RFP 2019-2021 Memo
NWEA Insights Report	*6:45 PM*	None *Assistant Superintendent, Ms. Christine Landwehrle, to update the Board on NWEA*	NWEA Insights Report

Data and Security Plan- Update	*7:05 PM*	None *Ms. Landwehrle and Director of Technology Mr. Bruce Chakrin to present Data and Security Plan*	Data Security and Data Privacy Guidelines Draft
Working Session- Strategic Plan Review	*7:15 PM*	None *Board to engage in a working session for Strategic Planning.*	None
Public Comment II of II	*7:50 PM*		None
Non- Public Session	*7:55 PM*	RSA 91 A:3 II ( )	
Meeting Adjourned	*8:00 PM*		

SAU #39 Board Meeting

Tuesday, April 16th, 2019

Meeting Minutes- Not Approved

Administrative Team: Adam Steel- Superintendent, Christine Landwehrle- Assistant Superintendent, Meg Beauchamp- Director of Student Services.

Amherst School Board: Elizabeth Kuzsma- Chair, John Glover- Secretary, Ellen Grudzien and Tom Gauthier.

Souhegan Cooperative School Board: Chair- Jim Manning, Vice Chair- Pim Grondstra, Secretary- Laura Taylor, Steve Coughlan, Amy Facey, and George Torres.

Mont Vernon School Board: Sarah Lawrence- Vice Chair, Stephen O'Keefe, Tom Driscoll and Jessica Hinckley.

Board Minutes: Danae Marotta

SHS Student Videographer: Shannon Hargreaves

Public: Community Members

I. Organizational Meeting-Call to Order

Superintendent, Mr. Adam Steel, called the meeting to order at 6:00PM.

II. Election of School Board Officers, Committee Appointments and Manifest Appointees

Mr. Steel then noted that he will be asking for nominations for SAU #39 Chair.

Mr. Steve Coughlan nominated Ms. Amy Facey for SAU #39 School Board Chair.

<u>The vote was unanimous, Ms. Facey is elected Chair of the SAU #39 School Board.</u>

Ms. Facey then asked for nominations for Vice-Chair.

Mr. Jim Manning nominated Mr. John Glover for Vice Chair.

Ms. Elizabeth Kuzsma nominated Mr. Steven O'Keefe as Vice Chair.

Ms. Facey called for a vote. 8 for Mr. O'Keefe, 6 for Mr. Glover.

<u>Mr. Stephen O'Keefe is elected Vice Chair of the SAU #39 Board.</u>

Mr. Jim Manning nominated Mr. John Glover for SAU #39 School Board Secretary.

The vote was unanimous.

<u>Mr. Glover is elected as Secretary of the SAU #39 Board.</u>

Manifest Appointees- Mr. Tom Gauthier and Ms. Jessica Hinckley

Draft

III. Appointments of School District Treasurer

<u>Ms. Elizabeth Kuzsma motioned to appoint Ms. C.J Butler as SAU #39 School District Treasurer. Ms. Sarah Lawrence seconded the motion. The vote was unanimous, motion passed.</u>

IV. Public Input

No Public Comment

V. Boards' Updates

<u>Mont Vernon School District</u>

Ms. Sarah Lawrence, Chair of the MVVSB, noted that Mr. Thomas Driscoll is back for a one-year term, and things are looking good with their budget

The Board thanked Ms. Lawrence.

<u>Amherst School District</u>

Ms. Elizabeth Kuzsma, Chair of the ASB, discussed that they approved how they are going to make their budget work with the default. At the last board meeting they got an update from Dr. Femia- Hou about future community based Social and Emotional Learning events.

The Board thanked Ms. Kuzsma.

<u>Souhegan Cooperative School District</u>

Mr. Jim Manning, Chair of the SCSB, noted that Mr. Grondstra is Vice-Chair and Ms. Taylor is Secretary.

Community Council is taking up the idea of weighted GPA and there is a lot of discussion about that. Second, the Constitutional Interpretation Committee is also doing deep work. That came from the idea that proposals get passed get lost, not feasible or too expensive.

He then invited people to stay for the SCSB meeting.

The Board thanked Mr. Manning.

VI. Reconfiguration Committee Update

Chair of the SAU #39 Reconfiguration Committee, Ms. Sarah Lawrence explained that they are doing regular meetings and they are digging into information and seeing what the first steps are.

Ms. Facey asked Mr. Steel if the Board Members needed an invite on the Trello Board.

Mr. Steel replied, yes, just let him know.

The Board thanked Ms. Lawrence.

VII. Superintendent's Report

Superintendent Steel noted that he has nothing for this evening as it is in tonight's discussion.

Draft

VIII. Consent Agenda

Superintendent Steel noted that the Draft Minutes should say March 21st 2019.

Mr. Pim Grondstra motioned to approve Consent Agenda items 1. Approve Minutes of March 21st, 2019 2. Approve Budget Transfers and 3. Q3 Finance Report. Mr. John Glover seconded the motion. 13 in favor, motion passed. Mr. Thomas Driscoll abstained.

IX. Policies Review

Assistant Superintendent, Ms. Christine Landwehrle, remarked that this is a first reading. The next section is for them to review and move to individual boards.

Mr. O'Keefe asked about Policy DC and if the SAU is able to borrow funds.

Mr. Steel replied that he believes that the SAU can Borrow funds. He then added that he will find out and get back to them for the next meeting.

Mr. Gauthier asked about Policies DBF and DBI.

Mr. Coughlan replied that he went over the "D" Policies with Finance Director, Ms. Katie Hannan.

Ms. Facey asked for other comments. She then noted that they will work on DBI and DBF and bring it back.

Mr. Coughlan added that DBI and DBF are the existing policies in Amherst and Mont Vernon.

Ms. Kuzsma suggested that they take DBJ as well.

Ms. Facey noted that they will be removing policies DBF, DBI and DBJ and sending back to the Policy Committee for further review.

Mr. Pim Grondstra motioned to move the Policies DA, DB, DBB, DBC, DC, DD, DEA, DFA, DG, DGA, DH, DI, DIA, DIAM, DID, EHAA, EHAB, and ADB /GBEC for a second reading. Ms. Elizabeth Kuzsma seconded the motion. The vote was unanimous, motion passed.

Ms. Facey noted that they will be moving to the other set of policies. These are policies that need to move to the individual boards.

Mr. Glover asked about the tables of retention periods EHB-R, does it need to be reviewed on a regular basis.

Superintendent Steel replied that some are governed by a specific statute.

Ms. Facey added that they will bring back Policy EHB-R to the Policy Committee for further review.

Mr. Pim Grondstra motioned to move policy ADB/GBEC to the Individual Boards. Mr. Tom Gauthier seconded the motion. The vote was unanimous, motion passed.

X. Strategic Planning

Draft

Superintendent Steel noted that the next Strategic Planning Meeting is Thursday, May 2 at the MVVS. What is included in the packet is a visual representation of a Portrait of a Graduate.

Ms. Landwehrle explained the work that they have completed with Vision of a Graduate. She then noted that the graphic combines the Mont Vernon and Amherst communities.

Mr. Manning asked about the term “Knowledge Constructor”.

Ms. Landwehrle replied that they had a long conversation about that. It is more about students building their own knowledge.

Ms. Facey asked for an update with Strategic Planning.

Mr. Steel reviewed that an entire SWOT analysis has been done, then and it has been put in a Current State Analysis Document from that document comes strategies. The Strategic Planning Committee will then give feedback at that meeting. That is why it is so important.

Ms. Grudzien added that she is in support of the language.

Mr. Glover noted that they want to be consistent.

Mr. Manning clarified that when you have a public facing document, you want language that people understand.

Ms. Lawrence asked Mr. Manning if he found something that makes more sense to him.

Discussion ensued over the language.

The Board thanked Superintendent Steel.

XI. Data and Security Update

Assistant Superintendent Landwehrle discussed that the ATOM Group, Portsmouth, NH, www.theatomgroup.com/#home pulled together a data analysis and the other big thing is the policy. They hope to have a draft planned and it would need to be approved by June.

Mr. Glover asked for time to debate and discuss.

Ms. Landwehrle noted that it would go out and the tech department and ideally it and the tech people need April break to work on the plan.

Ms. Taylor asked about the purpose.

Ms. Landwehrle replied the policy is meant around personally identifiable information. Anytime they are creating student log ins they want to make sure that is a safe place for students to be.

The Board thanked Ms. Landwehrle.

Ms. Facey reviewed the remaining board meeting dates.

Ms. Grudzien asked about a joint ASB and MVVSB meeting.

Mr. Steel replied that the two Board Chairs will meet with him.

Draft

XII. Non-Public Session

None

XIII. Meeting Adjourned

Mr. Stephen O'Keefe motioned to adjourn the meeting at 6:52PM. Mr. Pim Grondstra seconded the motion. The vote was unanimous, motion passed.

Draft

Consent Agenda Item #2

SCHOOL ADMINISTRATIVE UNIT #39
TOWN OF AMHERST, NH
Treasurer Report

March-2019

School Adminstrative Unit #39		
Town of Amherst, NH Monthly Report of the Treasurer		
as of 3/31/2019		
Cash on hand	**3/1/2019**	**$546,836.26**
Deposits		**$288,008.70**
AP-PR		**($244,826.12)**
Balance on hand	**3/31/2019**	**$590,018.84**

Filename: 2019-03-SAU39 Treasurer Report.xlsx
Month 3/1/2019

Catherine Jo Butler, Treasurer

Printed 3/31/2019

SAU#39
Monthly Reconciliation Report
Combined Accounts

March-19	Peoples United *1191 Cash Management	Peoples United *760 Municipal Checking	TOTAL
3/31/2019	$657,968.99	$10,000.00	$667,968.99
Deposits in Transit: (add)			
Outstanding Checks: (subtract)			
a) Accounts Payable		$(29,521.48)	
b) Payroll		$(48,428.67)	
c) Payroll Direct Deposit & IRS			
Total Outstanding		$(77,950.15)	$(77,950.15)
Reconciled Book Balance			$590,018.84
Balance from Treasurer's Journal			$590,018.84
Difference			-

Printed 3/31/2019

School Administrative Unit #39
Town of Amherst, NH
Treasurer's Cash Journal

Date	Deposits Description	Amount	Deposit Total	Date	Expenditures Description	Amount	Balance
3/1/2019	**Beginning Balance**						**$546,836.26**
3/6/2019	Deposit: Healthtrust	$0.66	$0.66	3/5/2019	Payroll Direct Deposit pp18 v6068	($34,201.69)	**$512,635.23**
3/18/2019	Deposit: ASD, MVSD	$140,975.70	$140,975.70	3/5/2019	Payroll Direct Deposit pp18 v6069	($3,684.07)	**$649,926.86**
3/20/2019	Deposit: SCSD	$83,810.60	$83,810.60	3/19/2019	Payroll Direct Deposit pp19 v6073	($34,113.36)	**$699,624.10**
				3/19/2019	Payroll Direct Deposit pp19 v6074	($3,662.82)	**$695,961.28**
				3/7/2019	Payroll IRS pp18 v6071	($6,308.00)	**$689,653.28**
				3/21/2019	Payroll IRS pp19 v6076	($6,333.36)	**$683,319.92**
				3/8/2019	Payroll 457 pp18 v6070	($2,207.72)	**$681,112.20**
				3/22/2019	Payroll 457 pp19 v6075	($2,207.59)	**$678,904.61**
				3/7/2019	Payroll pp18 v6072 ck17122-17122	($335.42)	**$678,569.19**
				3/21/2019	Payroll pp19 v6077 ck400000-400000	($335.42)	**$678,233.77**
				3/22/2019	Payroll v6078 ck400001-400002	($48,428.67)	**$629,805.10**
							$629,805.10
							$629,805.10
							$629,805.10
							$629,805.10
				3/14/2019	A/P v1702 ck17123-17144	($87,161.03)	**$542,644.07**
				3/28/2019	A/P v1703 ck400003-400020	($21,596.97)	**$521,047.10**
				3/13/2019	AP VOID ck16972	$5,750.00	**$526,797.10**
10/31/2018	Heartland Payment Services	$62,984.50	$62,984.50				**$589,781.60**
							$589,781.60
3/31/2019	Interest - Cash Management	$237.24	$237.24				**$590,018.84**
							$590,018.84
							$590,018.84
3/31/2019	**Ending Balances**	**$288,008.70**	**$288,008.70**			**($244,826.12)**	**$590,018.84**
					Payroll Direct Deposit	($92,718.61)	
					Payroll	($49,099.51)	
					AP	($103,008.00)	

Printed 3/31/2019

SAU39 Treasurer's Report
Unreconciled Check Register

Uncleared Transactions
SAU39 Checking 0760

Num	Date	Payee	C	Memo	Category	Amount
Expense Categories						
Payroll Ded						
400001	3/22/2019	HEALTHTRUST, INC.		6078	Payroll Ded	($31,649.37)
400002	3/22/2019	NEW HAMPSHIRE RETIREMENT SYSTEM		6078	Payroll Ded	($16,779.30)
Total Payroll Ded						($48,428.67)
Expense!						
17073	1/24/2019	MBG CONSULTING, LLC		1699	Expense!	($250.00)
17097	2/7/2019	MOULTON'S MARKET		1700	Expense!	($47.94)
17124	3/14/2019	ASCD		1702	Expense!	($30.46)
17127	3/14/2019	BEAUCHAMP, MARGARET		1702	Expense!	($34.99)
17128	3/14/2019	BUCKLEY DISPOSAL SERVICES		1702	Expense!	($34.00)
17129	3/14/2019	CANON SOLUTIONS AMERICA, INC.		1702	Expense!	($114.47)
17131	3/14/2019	EVERSOURCE		1702	Expense!	($2,985.97)
17132	3/14/2019	GOT INK 4U		1702	Expense!	($87.99)
17134	3/14/2019	LOWE'S		1702	Expense!	($51.66)
17135	3/14/2019	MONT VERNON SCHOOL DISTRICT		1702	Expense!	($3,898.00)
17136	3/14/2019	NHGFOA		1702	Expense!	($350.00)
17138	3/14/2019	SHRED-IT USA LLC		1702	Expense!	($39.03)
400003	3/28/2019	AMAZON.COM		1703	Expense!	($31.98)
400004	3/28/2019	AMHERST SCHOOL DISTRICT		1703	Expense!	($7,257.27)
400005	3/28/2019	BALSAMA, RICHARD		1703	Expense!	($500.00)
400006	3/28/2019	CONSOLIDATED COMMUNICATIONS, INC		1703	Expense!	($2,341.06)
400007	3/28/2019	Dodge, Porter B.		1703	Expense!	($274.28)
400008	3/28/2019	Maruca, Marie E.		1703	Expense!	($26.22)
400009	3/28/2019	MONT VERNON SCHOOL DISTRICT		1703	Expense!	($1,069.83)
400010	3/28/2019	NHASEA - ANNUAL LAW CONFERENCE		1703	Expense!	($400.00)
400011	3/28/2019	PENNICHUCK WATER WORKS, INC.		1703	Expense!	($83.43)
400012	3/28/2019	PICKUP PATROL		1703	Expense!	($17.00)
400013	3/28/2019	RIMOL, KAREN		1703	Expense!	($150.00)
400014	3/28/2019	SHRED-IT USA LLC		1703	Expense!	($41.76)
400015	3/28/2019	SOUHEGAN COOPERATIVE SCHOOL DIST		1703	Expense!	($5,028.38)
400016	3/28/2019	SOULE, LESLIE, KIDDER, SAYWARD		1703	Expense!	($196.00)
400017	3/28/2019	Steel, Adam A.		1703	Expense!	($3,300.46)
400018	3/28/2019	THE MASTER TEACHER, INC.		1703	Expense!	($167.70)
400019	3/28/2019	UNION LEADER CORPORATION		1703	Expense!	($487.49)
400020	3/28/2019	W.B. MASON CO., INC.		1703	Expense!	($224.11)
Total Expense!						($29,521.48)
Total Expense Categories						($77,950.15)
Grand Total						($77,950.15)

DA - FISCAL MANAGEMENT POLICY

The school board recognizes the important trust it has been given with the responsibility of managing public resources. As trustee of local, state, and federal funds allocated for use in public education, the board will be vigilant in fulfilling its responsibility to see that these funds are used wisely for achievement of the purposes to which they are allocated.

In SAU 39's fiscal management, the board seeks to achieve the following goals:

1. To engage in thorough advance planning, in order to develop budgets and to guide expenditures so as to achieve the greatest educational returns and the greatest contributions to the educational program in relation to dollars expended.

2. To establish levels of funding which will provide high quality education for the district's students.

3. To use the best available process for budget development and management.

4. To provide timely and appropriate information to all staff with fiscal management responsibilities.

5. To establish effective and efficient procedures for accounting, reporting, business, purchasing and delivery, payroll, payment of vendors and contractors, and all other areas of fiscal management.

6. To communicate noteworthy quality improvement and cost-controlling actions to the public and press.

First Reading: April 16, 2019

SAU 39 POLICY

DB – ANNUAL BUDGET

One of the primary goals of the Board is to secure adequate funds to carry out a high-level program of instruction.

The adopted annual budget is the financial outline of the educational program; it is the legal basis for the establishment of tax rates. The annual school budget process is an important function of District operations and should serve as a means to improve communications within the school organization and with the residents of the community.

The Superintendent will be responsible for preparing, and presenting to the Board for adoption, the annual budget. The Board expects the Superintendent to work closely with the principal(s), and other school and SAU administrators to satisfy the needs of the schools. The Principals and administrators will confer with appropriate staff in getting budgetary requests and information on requirements.

First Reading: April 16, 2019

SAU 39 POLICY

DBB--FISCAL YEAR

The fiscal year is defined as beginning on the first day of July and ending on the thirtieth day of June following.

SAU 39 POLICY

DBC – BUDGET PREPARATION

The Superintendent may establish procedures for the involvement of staff in the development of the budget proposal.

The Board will adopt guidelines and a schedule each year for the timely submission of the budget to the Board, and budget advisory committee.

First Reading: April 16, 2019

SAU 39 POLICY

DC--TAXING AND BORROWING AUTHORITY AND LIMITATION

No funds will be borrowed without the expressed approval of the school district electorate as determined by a vote of the school district at an annual or special school district meeting in accordance with the Municipal Finance Act, RSA Chapter 33.

First Reading: April 16, 2019

SAU 39 POLICY

DD--FUNDING PROPOSALS AND APPLICATIONS

The Superintendent is to apprise the Board of its eligibility for general or program funds and to make recommendations for Board action.

First Reading: April 16,2019

SAU 39 POLICY

DEA – REVENUES FROM LOCAL TAX SOURCES

The major share of all financial support for the Districts (and therefore the SAU) is raised by taxing property. Most of the financial support of public education, therefore, is subject to a direct vote of the people.

It is the responsibility of the Board to explain the objectives and needs of the schools to appropriate community bodies that have a role in school budget adoption, and to the voters of the District Town(s).

The Board, administration, and the professional staff will work with the taxpayers toward the solution of problems in the operational funding of the Schools.

The Board will:

Accept all available state funds to which the District or SAU is entitled by law or through rules of the State Board of Education, and

Accept all funds which are available providing there is a specific need for them and that matching funds required are available.

The Board may accept revenues on a case-by-case basis consistent with its goals, policies, and programs.

First Reading: April 16, 2019

SAU 39 POLICY

DFA – INVESTMENT POLICY

The Board authorizes the Treasurer, working in conjunction with the Superintendent and his/her designee and pursuant to RSA 197:23-a, to invest the funds of the District (or SAU) subject to the following objectives and standards of care.

OBJECTIVES

The three objectives of investment activities shall be safety, liquidity, and yield.

1. **Safety** of principal is the foremost objective in this policy. Investments shall be undertaken in a manner that seeks to ensure the preservation of capital by mitigating credit and interest rate risk. This will be accomplished by limiting the type of the investments and institutions to those stipulated by statute and fully covered by FDIC insurance or collateral approved pursuant to applicable law.
2. **Liquidity** of the investment portfolio shall remain sufficient to meet all operating requirements that may be reasonably anticipated.
3. **Yield.** The investment portfolio shall be designed with the objective of attaining a market rate of return throughout budgetary and economic cycles, taking into account the investment risk constraints and liquidity needs. Return on investment is of secondary importance compared to the safety and liquidity objectives described above.

STANDARDS OF CARE

1. **Prudence.** The standard of prudence to be used by the Treasurer and Superintendent, or his/her designee involved in the investment process, shall be the "prudent person" standard and shall be applied in the context of managing an overall portfolio.
2. **Ethics and conflicts of interest.** The Treasurer and Superintendent, or his/her designee involved in the investment process, shall refrain from personal business activity that could conflict with the proper execution and management of the investment program or that could impair their ability to make impartial decisions. The members of the Investment of Funds Committee shall disclose any material interests in financial institutions with which they conduct business. They shall further disclose any personal financial institutions with which they conduct business. They shall also disclose any personal financial/investment positions that could be related to the performance of the investment portfolio. Employees and officials shall subordinate their personal investment transactions to those of the School District, particularly with regard to the timing of purchases and sales.
3. **Internal Controls.** The Treasurer and Superintendent or his/her designee shall establish a system of internal controls, which shall be documented in writing. The internal controls shall be reviewed by an independent auditor.

   The investment of funds will be left to the discretion of a Committee consisting of the Treasurer, the Director of Finance and the Business Administrator without prior approval of the Board. This committee shall be guided by RSA 197:23-a.

DFA – INVESTMENT POLICY (continued)

The Board will review the investment policy annually as part of its Budget Assumptions.

First Reading: April 16, 2019

Legal References:

RSA 197:23-a, Treasurer's Duties
RSA 383:22, Public Deposit Investment Pool

SAU 39 POLICY

DG – DEPOSITORY OF FUNDS

All income payable to the school district and all revenue received will be deposited with the school treasurer, who will credit it to the appropriate account.

The treasurer shall have custody of all moneys belonging to the district and shall pay out the same only upon orders of the school board or upon orders of the 2 or more members of the school board empowered by the school board as a whole to authorize payments.

First Reading: April 16, 2019

SAU 39 POLICY

DGA – AUTHORIZED SIGNATURES

Checks drawn on the general fund or any special fund (with the exception of the activity fund) will require the signature of the school district treasurer or deputy treasurer.

First Reading: April 16, 2019

DH - BONDED EMPLOYEES AND OFFICERS

The Board requires that the treasurer and assistant treasurer be bonded. The District (or SAU) will arrange a public officials bond to cover the treasurer and each assistant, if any, in the amount of $100,000. It is the practice that any employee who administers student activity money shall be bonded.

Any employee who administers funds will be bonded appropriately. The District (or SAU) will arrange a blanket position bond, including a faithful performance endorsement, in the amount of $100,000 on all employees who administer funds.

First Reading: April 16, 2019

SAU 39 POLICY

DI – FISCAL ACCOUNTING AND REPORTING

The accounting system will be in conformance with the New Hampshire Financial Accounting Handbook published by the State Department of Education. An adequate system of encumbrance accounting will be maintained.

The following purposes must be satisfied by the accounting system:

1. **Administrative Control**: The financial records must be adequate to guide the making or deferring of purchases, the expanding or curtailing of programs, and the controlling of expenses. Current data should be immediately available and in such form that periodic summaries may be readily made from the data.

2. **Budget Preparation**: The financial records must be adequate to serve as a guide to budget estimates of subsequent years, and to hold expenditures to the amounts appropriated. Accounts are to be kept for each item for which separate budget estimates must be made. An adequate code of expenditure accounts will be used.

3. **Accounting for Stewardship**: The financial records must be adequate to show that those in charge have handled funds within the framework of law and in accordance with Board policy.

Financial records will provide the following information:

1. **For each account in the budget:** the appropriation, appropriation transfers, expenditures, encumbrances, and unencumbered balance.

2. **For each purchase order:** the name of vendor, description of the item involved, approval of the Business Administrator and designated approver, the amounts, the call for bids if required, and an abstract of the bids received. Purchase order sets will be pre-numbered and each set accounted for.

3. **For each purchase:** the purchase order information, plus the record of receipt and condition of goods, the invoice and the record of payment.

4. **For each income account:** the budget estimate, the estimates as revised periodically, the receipts to date, and the balance anticipated.

5. Reimbursement of expenditures will be credited to the appropriate previously expended account within the same fiscal year, or to Refund of Prior Year Expenditure in the next fiscal year.

First Reading: April 16, 2019

SAU 39 POLICY

DIA –FUND BALANCES

Government Accounting Standards Board (GASB) 54 Fund Balance Reporting and Governmental Fund Definitions shall be complied with as follows**:**

The policy shall only apply to governmental funds.

The following Fund Types will be used in reporting activity in governmental funds using the definitions provided by GASB Statement No. 54: General Fund, Special Revenue Fund, Capital Project Fund and Permanent Fund. All fund types may or may not be reported in any given reporting period, based on actual activity.

Fund balance shall be reported in the following categories using the definitions provided by GASB Statement No. 54: Nonspendable, Restricted, Committed, Assigned and Unassigned amounts. Fund balances shall only be used or returned in accordance with applicable New Hampshire law and/or Governmental Standards Board Statement 54 (GASB 54)

First Reading: April 16, 2019

Legal References:

RSA 32, Municipal Budget Law
RSA 33, Municipal Finance Act
RSA 35, Capital Reserve Funds
Governmental Standards Board Statement 54 (GASB 54)

SAU 39 POLICY

DIAM – BOARD REVIEW AND SIGNING OF MANIFESTS

The shall designate two of its members at the annual organizational meeting in March, or when required by change in membership, to review and sign each manifest and thereby attest to the review (See Policy DG).

Any questions or concerns the board reviewers may have concerning a manifest will be brought to the immediate attention of the business office.

First Reading: April 16, 2019

SAU 39 POLICY

DID – FIXED ASSETS & DURABLE GOODS INVENTORIES

To serve the functions of conservation and control, a running inventory of fixed assets which exceed $10,000 in purchase price and with a useful service life in excess of 5 years (excluding software licenses) will be maintained by the Superintendent's office.

An inventory of durable goods for each school (and the SAU) will be maintained. Changes in durable goods inventory will be maintained on an ongoing basis and shared with the Superintendent's office. Inventories shall be reviewed periodically for accuracy. Discrepancies shall be investigated.

First Reading: April 16, 2019

EHAA - COMPUTER SECURITY, E-MAIL AND INTERNET COMMUNICATIONS

Category: Priority/Required by Law

See also EGA

SAU 39 has established this policy with regard to access and disclosure of electronic data composed, stored, sent, or received by employees using SAU 39 computer system. This policy is designed to protect the safety and security of the SAU 39's computer systems including e-mail and Internet use.

SAU 39 intends to enforce the rules set forth below and reserves the right to change these rules at any time.

1. The computer hardware system, software and e-mail system are owned by SAU 39, and all messages or data composed, stored, sent, or received using the system are and remain the private property of SAU 39. They are not the property of the employee.

2. The computer and e-mail system is to be used for business purposes only. Personal business is unauthorized and should not be conducted on the system.

3. The electronic mail system may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job related solicitations.

4. SAU 39 prohibits discriminatory, harassing, or offensive materials in any form of media. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comments that offensively address someone's age, sexual orientation, religious or political beliefs, national origin, or disability.

5. The electronic mail system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

6. SAU 39 reserves, and intends to exercise without prior notice, the right to read, review, audit, intercept, access or disclose any and all information on an employee's computer system or messages created, received or sent over the electronic mail system for any purpose, even if coded or passworded.

7. The confidentiality of any message or data should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. The use of passwords for security does not guarantee confidentiality, or that SAU 39 will not retrieve it. All passwords must be disclosed to the computer administrator.

8. Any communications created, sent, or retrieved using e-mail may be read by individuals other than the intended recipient.

9. Notwithstanding SAU 39's right to retrieve and monitor any e-mail messages, such messages should be treated as confidential by other employees and accessed only by the

intended recipient. Employees are not authorized to retrieve or read any e-mail that is not sent to them. Any exception to this policy must receive prior approval by the Superintendent.

10. Any employee who violates this policy or uses the computer system or electronic mail system for improper purposes shall be subject to discipline up to and including discharge.

11. SAU 39 has the authority to terminate or limit access to any program at any time.

12. Personal disks cannot be used on the system unless pre-authorized by the computer coordinator.

13. SAU 39 will take all necessary measures to maintain student privacy relative to SAU 39's website, online information and storage of student personally identifiable information, as required by state and federal law.

First Reading: April 16, 2019

SAU 39 Policy

EHAB - DATA GOVERNANCE AND SECURITY

Category: Priority/Required by Law

Related Policies EHAA, EHB, GBEBD, GBEF,
IHBH, JICJ, JICL, JICM, KD, & KDC

To accomplish SAU 39's mission and comply with the law, the SAU 39 must collect, create and store information. Accurately maintaining and protecting this data is important for efficient SAU 39 operations, compliance with laws mandating confidentiality, and maintaining the trust of the SAU 39's stakeholders. All persons who have access to SAU 39 data are required to follow state and federal law, SAU 39 policies and procedures, and other rules created to protect the information.

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

A. Definitions

Confidential Data/Information - Information that the SAU 39 is prohibited by law, policy or contract from disclosing or that the SAU 39 may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information regarding students and employees.

Critical Data/Information - Information that is determined to be essential to SAU 39 operations and that must be accurately and securely maintained to avoid disruption to SAU 39 operations. Critical data is not necessarily confidential.

B. Data and Privacy Governance Plan - Administrative Procedures.

1. Data Governance Plan. The Superintendent, in consultation with the SAU 39 Information Security Officer ("ISO") (see paragraph C, below) shall create a Data and Privacy Governance Plan ("Data Governance Plan"), to be presented to the Board no later than June 30, 2019. Thereafter, the Superintendent, in consultation with the ISO, shall update the Data Governance Plan for presentation to the Board no later than June 30 each year.

The Data Governance Plan shall include:

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

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

(c) Policies and procedures for access to data and protection of privacy for students and

staff including acceptable use policy for applications, digital tools, and extensions used on District hardware, server(s) or through the District network(s);

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

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

2. Policies and Administrative Procedures. The Superintendent, in consultation with the ISO, is directed to review, modify and recommend (policies) create (administrative procedures), where necessary, relative to collecting, securing, and correctly disposing of SAU 39 data (including, but not limited to Confidential and Critical Data/Information, and as otherwise necessary to implement this policy and the Data Governance Plan. Such policies and/or procedures will may or may not be included in the annual Data Governance Plan.

C. Information Security Officer.

The Director of Technology is hereby designated as the SAU 39's Information Security Officer (ISO) and reports directly to the Superintendent or designee. The ISO is responsible for implementing and enforcing SAU 39's security policies and administrative procedures applicable to digital and other electronic data, and suggesting changes to these policies, the Data Governance Plan, and procedures to better protect the confidentiality and security of SAU 39's data. The ISO will work with the both SAU 39 and building level administrators and Data managers (paragraph E, below) to advocate for resources, including training, to best secure the SAU 39's data.

The Network Administrator is the SAU 39's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

D. Responsibility and Data Stewardship.

All SAU 39 employees, volunteers and agents are responsible for accurately collecting, maintaining and securing SAU 39 data including, but not limited to, Confidential and/or Critical Data/Information.

E. Data Managers.

All SAU 39 administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the SAU 39's data inventory. Data managers will monitor employee access to the information to ensure that confidential information is accessed only by employees who need the information to provide services to the SAU 39 and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISO in enforcing SAU 39 policies and procedures regarding data management.

F. Confidential and Critical Information.

The SAU 39 will collect, create or store confidential information only when the Superintendent or designee determines it is necessary, and in accordance with applicable law. The District will provide access to confidential information to appropriately trained SAU 39 employees and volunteers only when the SAU 39 determines that such access is necessary for the performance of their duties. SAU 39 will disclose confidential information only to authorized SAU 39

contractors or agents who need access to the information to provide services to SAU 39 and who agree not to disclose the information to any other party except as allowed by law and authorized by the SAU 39.

SAU 39 employees, contractors and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise. The ISO or designee will investigate immediately and take any action necessary to secure the information, issue all required legal notices and prevent future incidents. When necessary, the Superintendent, ISO or designee is authorized to secure resources to assist SAU 39 in promptly and appropriately addressing a security breach.

Likewise, SAU 39 will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure.

SAU 39 staff, volunteers, contractors and agents who are granted access to critical or confidential information/data are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of such confidential or critical data/information. All individuals using confidential and critical data/information will strictly observe all administrative procedures, policies and other protections put into place by the District including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information no longer needed in a confidential and secure manner.

G. Using Online Services and Applications.

SAU 39 staff members are encouraged to research and utilize online services or applications to engage students and further the SAU 39's education mission. SAU 39 employees, however, are prohibited from installing or using applications, programs or other software, or online system/website, that either stores, collects or shares confidential or critical data/information, until the ISO approves the vendor and the software or service used. Before approving the use or purchase of any such software or online service, the ISO or designee shall verify that it meets the requirements of the law, Board policy, and the Data Governance Plan, and that it appropriately protects confidential and critical data/information. This prior approval is also required whether or not the software or online service is obtained or used without charge.

H. Training.

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

I. Data Retention and Deletion.

The ISO or designee shall establish a retention schedule for the regular archiving and deletion of data stored on SAU 39 technology resources. The retention schedule should comply with, and be

incorporated into the data/record retention schedule established under Policy EHB and administrative procedure EHB-R, including but not limited to, provisions relating to Litigation and Right to Know holds as described in Policy EHB.

J. Consequences

Employees who fail to follow the law or SAU 39's policies or procedures regarding data governance and security (including failing to report) may be disciplined, up to and including termination. Volunteers may be excluded from providing services to SAU 39. SAU 39 will end business relationships with any contractor who fails to follow the law, SAU 39 policies or procedures, or the confidentiality provisions of any contract. In addition, SAU 39 reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

SAU 39 may suspend all access to data or use of SAU 39 technology resources pending an investigation. Violations may result in temporary, long-term or permanent suspension of user privileges. SAU 39 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 SAU 39.

Any attempted violation of SAU 39's policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

First reading: April 16, 2019

Legal References:

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

SAU 39 Policy

ADB/GBEC - DRUG-FREE WORKPLACE & DRUG-FREE SCHOOLS

Related Policy: JICH

A. Drug-Free Workplace

1. All SAU 39 workplaces are drug- and alcohol-free. All employees and contracted personnel are prohibited from:

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

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

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

3. For purposes of this policy, "workplace" shall mean the site for the performance of work, and will include at a minimum any SAU 39 building or grounds owned or operated by SAU 39, any school-owned vehicle, and any other school-approved vehicle used to transport students to and from school or school activities. It shall also include off-school property during any school-sponsored or school-approved activity, event or function such as a field trip or athletic event where students are under the jurisdiction, care or control of SAU 39.

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

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

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

5. In order to make employees aware of dangers of drug and alcohol abuse, SAU 39 will endeavor to:

   a. Provide each employee with a copy of SAU 39 drug- and alcohol-free workplace policy;

   b. Post notice of SAU 39 drug- and alcohol-free workplace policy in a place where other information for employees is posted;

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

B. SAU 39 Action Upon Violation of Policy

An employee who violates this policy may be subject to disciplinary action; up to and including termination of employment. Alternatively, the Board may require an employee to

successfully complete an appropriate drug- or alcohol-abuse, employee-assistance rehabilitation program.

The Board will take disciplinary action with respect to an employee convicted of a drug offense in the workplace, within thirty (30) days of receiving notice of a conviction. Should SAU 39 employees or contracted personnel be engaged in the performance of work under a federal contract or grant, or under a state contract or grant, the Superintendent will notify the appropriate state or federal agency from which the District receives contract or grant moneys of an employee/contracted personnel's conviction, within ten (10) days after receiving notice of the conviction.

The processes for disciplinary action shall be those provided generally to other misconduct for the employee/contractor personnel as may be found in applicable collective bargaining agreements, individual contracts, School Board policies, contractor agreements, and or governing law. Disciplinary action should be applied consistently and fairly with respect to employees of SAU 39 and/or contractor personnel as the case may be.

C. Drug-Free School Zone

Pursuant to New Hampshire's "Drug-Free School Zone" law (RSA Chapter 193-B), it is unlawful for any person to manufacture, sell prescribe administer, dispense, or possess with intent to sell, dispense or compound any controlled drug or its analog, within a "drug-free school zone". The Superintendent is directed to assure that SAU 39 is and remains in compliance with the requirements of RSA 193-B, I, and N.H. Ed. Part 316 with respect to establishment, mapping and signage of the drug-free zone around each school of SAU 39.

D. Implementation and Review

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

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

First reading: April 16, 2019

Legal References:

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

Policies First Reading: DBF, DBI, DBJ, EHB,EHB-R and KE/KEB

DBF – BUDGET REVIEW / HEARING / ADOPTION

The budget will be made available to the budget advisory committee, the press, and the public at the same time the Superintendent presents the budget to the board.

The budget shall be presented through public hearings and adopted as prescribed by the applicable RSAs.

DBI – BUDGET IMPLEMENTATION

The Superintendent will establish procedures for budget implementation, control, and reporting.

RSA 32:10, Transfer of Appropriations
NH Code of Administrative Rules Section Ed. 302:02 (e) (j) (o,) Substantive Duties of the Superintendent

DBJ – TRANSFER OF APPROPRIATIONS

It is the intent of the Board to limit its spending to the amount specified for each functional area. However, transfer of funds between functional areas may be permitted if approved by the Board upon request from the Superintendent. Excess funds may not be transferred from the unemployment compensation line item.

All transfers will be in accordance with the requirements of RSA 32:10 and implemented by internal procedures set forth by the Superintendent.

RSA 32:10, Transfer of Appropriations

RSA 282-a:71, III, Unemployment Compensation

EHB – DATA/RECORDS RETENTION

Related Policies: EH, EHAB, JRA, & JBJ
See also: EHB-R (Records Retention Schedule)

The Superintendent shall develop procedures for a records retention system that is in compliance with RSA 189:29-a and Department of Education regulations, and also addresses retention/destruction of all other records which are not subject to specific statutes or regulations. The procedures should ensure that all pertinent records are stored safely and are stored for such durations as are required by law. The Superintendent shall develop procedures necessary to protect individual rights and preserve confidential information.

This policy shall apply to all district records, irrespective of the specific medium of the record, i.e., paper, electronic, digital, cloud, etc.

A. <u>Special Education Records</u>

1. Upon a student's graduation from high school, his or her parent(s)/guardian(s) may request in writing that the District destroy the student's special education records, including any final individualized education program.

2. The parent(s)/guardian(s) may, at any time prior to the student's twenty-sixth birthday, request, in writing, that the records be retained until the student's thirtieth birthday.

3. Absent any request by a student's parents to destroy the records prior to the twenty-sixth birthday, or to retain such records until the student's thirtieth birthday, the District shall destroy a student's records and final individualized education program within a reasonable time after the student's twenty-sixth birthday, provided that all such records be destroyed by the student's thirtieth birthday.

4. A permanent record of a student's name, address, and phone number, his or her grades, attendance record, classes attended, grade level completed, and year completed may be maintained without time limitation. 34 CFR 300.624.

5. The District shall provide parents/guardians, or where applicable, the adult student, with a written notice of the District's document destruction policies upon the student's graduation with a regular high school diploma or at the transfer of rights, whichever occurs first.

6. The District shall provide public notice of its document destruction policy at least annually.

B. <u>Litigation Hold</u>

On receipt of notice from legal counsel representing the District in that a litigation hold is required, the routine destruction of governmental records, including paper and electronic or digital records, which are or may be subject to the litigation hold shall cease. The destruction of records subject to a litigation hold shall not resume until the District has received a written directive from legal counsel authorizing resumption of the routine destruction of those records in accordance with the retention requirements of this policy and the associated procedures.

C. Right-to-Know Request Hold

On receipt of a Right-to-Know law request to inspect or copy governmental records, the Superintendent shall cease any destruction of governmental records which are or may be the subject of the request. The records shall be retained regardless of whether they are subject to disclosure under RSA Chapter 91-A, the Right-to-Know law. If a request for inspection is denied on the grounds that the information is exempt under this chapter, the requested material shall be preserved for no less than ninety (90) days and until any lawsuit pursuant to RSA 91-A:7-8 has been finally resolved, all appeal periods have expired, and a written directive from legal counsel representing the District authorizing destruction of the records has been received.

RSA 91-A, Right to Know Law
RSA 189:29-a, Records Retention and Disposition
NH Code of Administrative Rules, Section Ed 306.04(a)(4), Records Retention
NH Code of Administrative Rules, Section Ed 306.04(h), Records Retention
NH Code of Administrative Rules, Section Ed. 1119.01, Confidentiality Requirements
20 U.S.C. 1232g, Family Educational Rights and Privacy Act (FERPA)

EHB-R – LOCAL RECORDS RETENTION SCHEDULE

See Board Policy: EHB
Related Policies: EH, EHAB, JRA, and JBJ

The following schedule shall apply to all records obtained, created or maintained by the District, irrespective of the specific medium of the record, i.e., paper, electronic, digital, cloud, etc.

A. Special Education Records

1. Upon a student's graduation from high school, his or her parent(s)/guardian(s) may request in writing that the District destroy the student's special education records, including any final individualized education program.

2. The parent(s)/guardian(s) may, at any time prior to the student's twenty-sixth birthday, request, in writing, that the records be retained until the student's thirtieth birthday.

3. Absent any request by a student's parents to destroy the records prior to the twenty-sixth birthday, or to retain such records until the student's thirtieth birthday, the District shall destroy a student's records and final individualized education program within a reasonable time after the student's twenty-sixth birthday, provided that all such records be destroyed by the student's thirtieth birthday

4. A permanent record of a student's name, address, and phone number, his or her grades, attendance record, classes attended, grade level completed, and year completed may be maintained without time limitation. 34 CFR 300.624.

5. The District shall provide parents/guardians, or where applicable, the adult student, with a written notice of the District's document destruction policies upon the student's graduation with a regular high school diploma or at the transfer of rights, whichever occurs first.

6. The District shall provide public notice of its document destruction policy at least annually.

B. Litigation Hold

On receipt of notice from legal counsel representing the District that a litigation hold is required, the routine destruction of governmental records, including paper and electronic records, which are or may be subject to the litigation hold shall cease. The destruction of records subject to a litigation hold shall not resume until the district has received a written directive from the attorney representing the district authorizing resumption of the routine destruction of those records.

C. Right-to-Know Request - Hold

On receipt of a Right-to-Know law request to inspect or copy governmental records, the Superintendent shall cease any destruction of governmental records which are or may be the subject of the request. The records shall be retained regardless of whether they are subject to disclosure under RSA Chapter 91-A, the Right-to-Know law. If a request for inspection is denied on the grounds that the information is exempt, the requested material shall be preserved for no less than 90 days and until any lawsuit pursuant to RSA 91-A:7-8 has been finally resolved, all appeal periods have expired, and a written directive from the attorney

representing the District authorizing destruction of the records has been received.

D. Electronic Records

For legal purposes, electronic records and communications are no different than paper documents. The state law on preservation of electronic records, RSA 33-A:5-a Electronic Records, does not explicitly apply to school districts, but does provide guidance: "Electronic records as defined in RSA 5:29, VI and designated on the disposition schedule under RSA 33-A:3-a to be retained for more than 10 years shall be transferred to paper or microfilm, or stored in portable document format/archival (PDF/A) on a medium from which it is readily retrievable. Electronic records designated on the disposition schedule to be retained for less than 10 years may be retained solely electronically if so approved by [Superintendent as the party] responsible for the records. The [Superintendent] is responsible for assuring the accessibility of the records for the mandated period." [Italics represent modified language to reflect Superintendent's responsibility for record retention and access.]

E. Retention Period Schedule

The following schedule shall apply to all records obtained, created or maintained by the District, irrespective of the specific medium of the record, i.e., paper, electronic, digital, cloud, etc.

Type of Record	**Retention Period**	**Statute, Rule, or other legal authority** ***If none listed, retention period is a recommendation (see end note)***
Business Records		
Accident Reports - Employee	Term of employment, plus 6 years	
Accident Reports - Student	Age of majority, plus 6 years	
Accounts Receivable	Until audited, plus 1 year	RSA 33-A:3-a
Annual Audit	Permanent	RSA 33-A:3-a (10 years)
Annual Report (District), Warrants, Annual Meeting Minutes, Budgets (District & SAU)	Permanent	RSA 33-A:3-a
Application for Federal Grants	5 years	20 U.S.C. 1232f., (three years after the completion of the activity for which the funds are used) other authorities may apply
Architectural Plans	Permanent	

Type of Record	**Retention Period**	**Statute, Rule, or other legal authority** ***If none listed, retention period is a recommendation (see end note)***
Asbestos Removal	Permanent	
Bank Deposit Slips	6 years	RSA 33-A:3-a
Bonds and continuation certificates	Permanent	RSA 33-A:3-a (expiration plus 2 years)
Budget Worksheets	End of budget year, plus 1 year	
Cash receipts, disbursement records, checks	Until Audited and at least 6 years after last entry	RSA 33-A:3-a
Child Labor Permits	1 year	
Work-study	3 years from date of enrollment	29 C.F.R. §570.37
Construction Contracts, Capital projects, fixed assets that require accountability after acquired*	Life of contract, building, asset plus 20 years	RSA 33-A:3-a (Life of project/asset)
Engineering Surveys	Permanent	
Unsuccessful bids	Life of contract plus 3 years	RSA 33-A:3-a (Completion of project, plus one year)
Certified Educator	Permanent	
COBRA Notices	6 years from date of issue	42 U.S.C. 300bb-1, *et. seq.(3 years)* ERISA 29 U.S.C. §1027 (6 years)
Collective Bargaining Agreements	Permanent	
Correspondence for Business transactions*	Life of subject matter plus 4 years	
Correspondence - General	3 years or longer when historic/useful	
Correspondence Transitory	As needed for reference	RSA 33-A:3-a
Deeds	Permanent	
District Meeting Minutes & Warrant	Permanent	

Type of Record	Retention Period	Statute, Rule, or other legal authority *If none listed, retention period is a recommendation (see end note)*
Insurance policies	Permanent	RSA 33-A:3-a
Notes (loan documents)	Until paid, Audited, plus 3 years	RSA 33-A:3-a
Student Activities Records/Accounts	Until Audited, plus 6 years	RSA 33-A:3-a (bank deposit slips and statements 6 years)
Enrollment Reports: Fall Reports A12A (RSA 189:28)	Permanent	
Enrollment Reports: Pupil Registers	Permanent	RSA 189:27-b
Enrollment Reports: Resident Pupil Membership Forms	14 years	
Enrollment Reports: School Opening Reports	3 years	
Enrollment Reports: Statistical Report A-3 (RSA 189:28)	Permanent	
Federal Projects Documents	5 years after submission of final audit report and documentation for expenditures, unless there is an ongoing audit	Review specific project/grant program requirements. 20 U.S.C. 1232f, (three years after the completion of the activity for which the funds are used), other authorities may apply
FICA Reports – monthly	7 years	
Fixed Trip Requests/Confirmation	1 year	
Fixed Assets Schedule	Permanent/as updated	
Form C-2 Unemployment	6 years	
Wage Report (DES 100)	6 years	
Invoices*	3 years*	Until Audited, plus 1 year

Type of Record	Retention Period	Statute, Rule, or other legal authority *If none listed, retention period is a recommendation (see end note)*
MS-22 Budget Form	6 years	
MS-23 Budget Form	6 years	
MS-25 Budget Form	Permanent	
Minutes of Board Meetings, Board Committees	Permanent	RSA 91-A:2, II, RSA 33-A:3-a
Purchase Orders*	Until Audited, plus 1 year	
Request for Payment Vouchers*	Until Audited, plus 1 year	
Requisitions*	Until Audited, plus 1 year	
Retirement Reports – Monthly	1 year	
Timecards: Bus Drivers	5 years	Lab 803.03. Notification and Records no less than 4 years
Timecards: Custodial	5 years	Lab 803.03. Notification and Records no less than 4 years
Timecards: Secretarial	5 years	Lab 803.03. Notification and Records no less than 4 years
Timecards: Substitute Teachers pay slips	5 years	Lab 803.03. Notification and Records no less than 4 years
Payroll Records	6 years	RSA 33-A:3-a Audited, plus 2 year 29 C.F.R. §1627.3 (3 years) ADEA: 29 U.S.C. §626, 29 CFR Part 1602 (2 years from job action); 29 C.F.R § 825.500 FMLA, 29 U.S.C.§2616, 3 years
Travel Reimbursements*	3 years*	Until Audit, plus 1 year
Treasurer's Receipts – canceled checks	6 years	
Treasurer's Report	6 years	

Type of Record	Retention Period	Statute, Rule, or other legal authority *If none listed, retention period is a recommendation (see end note)*
Vocational Education: AVI Forms	1 year	
Vocational Education: Vocational Center Regional Contracts	20 years	
Vocational Education: Federal Vocational Forms*	6 years	
Vouchers Manifests*	Until Audit, plus 1 year	
Tax Forms: W-2's, 1099 *	7 years	Keep all records of employment taxes for at least four years after filing the 4th quarter for the year. – 26 C.F.R § 31.6001-1 (e)(2)(tax advisors say 7 years)
Tax Forms: W-4 Withholding Exemption Certificate	7 years	Keep all records of employment taxes for at least four years after filing the 4th quarter for the year. – 26 C.F.R § 31.6001-1 (e)(2) (tax advisors say 7 years)
Tax Forms: W-9	7 years	Keep all records of employment taxes for at least four years after filing the 4th quarter for the year. – 26 C.F.R § 31.6001-1 (e)(2) (tax advisors say 7 years)
Tax Forms: 941-E Quarterly Taxes	7 years	Keep all records of employment taxes for at least four years after filing the 4th quarter for the year. – 26 C.F.R § 31.6001-1 (e)(2) (tax advisors say 7 years)
Personnel Records	Term of Employment, plus 50 years	RSA 33-A:3-a. Retirement or termination, plus 50 years
Application for employment - Successful	Term of Employment, plus 50 years	RSA 33-A:3-a Unsuccessful applicants: current year, plus 3 years.
Attendance Records: Leaves	3 years	Family Medical Leave Act – 3 years

Type of Record	Retention Period	Statute, Rule, or other legal authority *If none listed, retention period is a recommendation (see end note)*
Attendance Records: Request for Leaves	1 year	
Class Observation Forms	1 year	
Criminal Record Check: No criminal record	Destroy immediately after review	RSA 189:13-a (Superintendent only)
Criminal Record Check: Criminal record	Destroy within 30 days of receipt	RSA 189:13-a (Superintendent only)
Civil Rights Forms, Discrimination claims, accommodation under ADA, information used for EEO-5 report, EEO-5 report	6 years	29 C.F.R. §1602.40; 42 U.S.C. 12117; 42 U.S.C. § §§ 2000e-8-2000e-12; 42 U.S.C. § 2000ff-6; (final disposition, 2 years, 3 years)
Deferred Compensation plans	7 years	RSA 33-A:3-a
Dues Authorization	Term of Employment, plus 50 years	RSA 33-A:3-a. – Personnel record
Employment test papers with results	One year from date of personnel action	29 C.F.R. §1627.3
Evaluations	Term of Employment, plus 50 years	RSA 33-A:3-a. – Personnel record
HIPPA Documentation	Term of Employment, plus 50 years	RSA 33-A:3-a. – Personnel record HIPPA: 45 C.F.R. §164,316(b) & .530(j) – 6 years. HITECH 42 U.S.C. §17938
Labor-PELRB actions	Permanent	RSA 33-A:3-a
Labor Negotiations	Permanent	RSA 33-A:3-a
Legal Actions - lawsuits	Permanent	RSA 33-A:3-a
Medical Benefits Application	Term of Employment, plus 50 years	RSA 33-A:3-a. – Personnel record

Type of Record	Retention Period	Statute, Rule, or other legal authority *If none listed, retention period is a recommendation (see end note)*
Medical exams, Physical examinations used for personnel action	Term of Employment, plus 50 years	29 C.F.R. §1627.3(One year from date of personnel action) RSA 33-A:3-a. – Personnel record 29 C.F.R. §1910.1020 (term of employment plus 30 years)
Oaths of Office	Permanent	RSA 33-A:3-a Term, plus 3 years
Promotion, demotion, transfer, selection for training, layoff, recall, or discharge	Term of Employment, plus 50 years	29 C.F.R. §1627.3 (1 year from date of action) RSA 33-A:3-a. – Personnel record
Recruitment Documents	One year from date of personnel action	29 C.F.R. §1627.3
Re-employment Letter of Assurance	Term of Employment, plus 50 years	RSA 33-A:3-a. – Personnel record
Retirement application	Term of Employment, plus 50 years	RSA 33-A:3-a. – Personnel record
School Bus Driver Drug Tests – positive results & records of administration of test	5 years	49 C.F.R. §382.401; 49 C.F.R. § 40.333
School Bus Driver Drug tests – negative & cancelled	1 year	49 C.F.R. §382.401
Separation from Employment Form/Letter	Term of Employment, plus 50 years	RSA 33-A:3-a. – Personnel record
Settlement agreements, even if in anticipation of a lawsuit	Permanent	RSA 91-A:4, VI (10 years)
Staff Development Plan	Term of Employment, plus 50 years	Term of Employment, plus 50 years
Substitute Teacher Lists	7 years	
Student Records:		

Type of Record	**Retention Period**	**Statute, Rule, or other legal authority** ***If none listed, retention period is a recommendation (see end note)***
Applications for Free/Reduced Lunch	6 years	
Assessment Results	Permanent	Ed 306.04 Policy Development, (h) complete and accurate records of students' attendance and scholarship be permanently kept and safely stored in a fire-resistant file, vault, or safe.
Attendance	Permanent	Ed 306.04 Policy Development, (h) complete and accurate records of students' attendance and scholarship be permanently kept and safely stored in a fire-resistant file, vault, or safe.
Disciplinary Records	Term of Enrollment, plus 3 years	
Early Dismissal	1 year	
Emergency Information Form	1 year/as updated	
Grades	Permanent	Ed 306.04 Policy Development, (h) complete and accurate records of students' attendance and scholarship be permanently kept and safely stored in a fire-resistant file, vault, or safe.
Health and Physical Records	Term of Enrollment, plus 3 years	
Immunization Record	Term of Enrollment, plus 3 years	
Log of requests for access to education records	As long as the education record is retained	FERPA 20 U.S.C. §1232g (b)(4)(A)
Medical Reports	Term of Enrollment, plus 3 years	
Registration Form	Term of Enrollment, plus 3 years	
Student Handbook	1 copy of each edition, Permanent	

Type of Record	Retention Period	Statute, Rule, or other legal authority *If none listed, retention period is a recommendation (see end note)*
Transcripts	Permanent	Ed 306.04 Policy Development, (h) complete and accurate records of students' attendance and scholarship be permanently kept and safely stored in a fire-resistant file, vault, or safe.
Internal Records:		
Child Abuse Reports/Allegations	Permanent	
Criminal Investigation	Permanent	
Personnel Investigations	Permanent	
Sexual Harassment	Permanent	
Records Management, transfer to storage or disposal	Permanent	RSA 33-A:3-a (summary report of what category of records, for what range of dates, was put in storage or destroyed)
Vehicle maintenance	Life of vehicle, plus 3 years	RSA 33-A:3-a

* Note regarding records relating to federal funds (items marked with "*"): Before any records related to federal funds are destroyed the requirements of the General Education Provisions Act (GEPA) 20 U.S.C. 1232f shall be observed. Namely, that statute requires that district "shall keep records which fully disclose the amount and disposition by the recipient of [federal] funds, the total cost of the activity for which the funds are used, the share of that cost provided from other sources, and such other records as will facilitate an effective financial or programmatic audit . . . . for three years after the completion of the activity for which the funds are used." Therefore, to the extent that the below schedule, or other authorities, suggest that a purchase order, with accompanying documentation, may need to be retained only until the records are audited, plus 1 year, if the purchase is in part or in whole with federal funds the record must be retained for three years after the completion of the activity for which the funds are used, a much longer period of time.

End Note: Where different retention periods are required or recommended by different sources of legal authority, the longest retention period is listed in the retention period column, but the shorter period is cited in the statue, rule, or other legal authority column with the source of legal authority.

The recommended retention periods, except where another statute or rule are cited, are based on the New Hampshire requirements for municipalities as set forth in RSA 33-a:3-a where a category of records is listed in that statute which is not addressed in school law, consideration of the civil statutes of limitation in New Hampshire, and the guidance last issued several years ago by the New Hampshire Department of Education.

The retention period is a minimum. Unless destruction is required by law, where governmental records have historical value or other considerations warrant retention, the records may be retained for a longer period or permanently.

KE/KEB- PUBLIC COMPLAINTS ABOUT SCHOOL MATTERS, PERSONNEL, EMPLOYEES, STUDENTS OR ADMINISTRATION

Any complaint presented to the Board about school matters, personnel, employees, students or administration, will be referred back to the Superintendent. The Board will not hear or review complaints until such complaints have first been brought forth through the appropriate and applicable administrative procedures and the Superintendent or his/her designee has had a reasonable opportunity to seek to resolve the complaint.

The Board may decline to hear any complaint, which will interfere with its ability to serve as an impartial trier of fact in any related student or personnel matter. This complaint procedure shall not supersede or modify any right held by employees of the District under federal law, state law, contract, or collective bargaining agreement.

To the extent it is deemed appropriate by the Superintendent, the individual who is the subject of the complaint may be advised of the nature of the complaint and may be given an opportunity for explanation, comment, and presentation of the facts. The Superintendent shall seek to resolve the matter and report to the Board.

The Board believes that complaints and grievances are best handled and resolved by the parties directly concerned. Therefore, the proper channeling of complaints and/or grievances will be as follows:

1. Teacher
2. Principal
3. Superintendent
4. School Board

When any complaint is made directly to an individual Board member, the procedure outlined below shall be followed:

1. If the member of the public will not personally present the complaint to the appropriate level, the Board member shall then ask that the complaint be written and signed. The Board member will then refer the complaint to the Superintendent to be channeled appropriately.

2. If the person making a complaint at the Superintendent level believes that a satisfactory reply has not been received, he or she may request that the Board hear the complaint. The Board will hear and act upon the complaint only by majority vote. The Board may decline to act on any complaint which, in its sole judgment, would interfere with the Superintendent's ability to properly administer the district. If the Board does hear and act upon the complaint, all Board decisions shall be final.

3. If the Board decides, in accord with Paragraph Two, to hear and act upon a complaint that pertains to personnel, employee, student or administrative matters, it shall determine

whether the complaint shall be heard in public or non-public session in accord with RSA 91-A:3 and the laws pertaining to student and family privacy rights. The Board shall also determine whether it is appropriate to inform the individual who is the subject of the complaint of the meeting and to provide said individual with further opportunity for explanation, comment, and presentation of the facts to the Board.

4. If the Superintendent is the subject of the complaint, the SAU #39 Board shall determine whether the complaint should be heard in public or non-public session in accord with RSA 91-A:3. The SAU #39 Board may, to the extent it is appropriate, advise the Superintendent of the nature of the complaint and may give the Superintendent an opportunity for explanation, comment, and presentation of the facts.

MEMO

School Administrative Unit 39
1 School Street
P.O. Box 849
Amherst, NH 03031
Phone: 603-673-2690
Fax: 603-672-1786

Date: **4/12/2019**

To: **Adam Steel, Superintendent**

From: **Katie Hannan, Finance Director**

Re: **Financial Audit Recommendation**

On March 4, 2019 I submitted the attached Request for Proposal for annual financial auditing services for SAU #39 and the Amherst, Mont Vernon and Souhegan Cooperative School Districts. These requests were emailed directly to the following three firms that have provided us auditing services in the past- Melanson Heath & Company PC, Vachon Clukay & Co PC, and Plodzik & Sanderson PA, in addition to being posted on our website.

The RFP called for proposals to be submitted by March 20, 2019 at 3pm. All three of the above firms submitted a proposal on time. The proposed costs for each firm are attached to this memo.

At this time, it would be in the best interest of the Districts to remain with our current auditors, Plodzik & Sanderson PA. There is a negligible price difference between Plodzik and Vachon Clukay. Plodzik has been our auditor for the last 3 years, and Vachon was our auditor for the prior 6 years.

	SAU #39				Amherst		
	Plodzik & Sanderson, PA	Vachon	Melanson Heath		Plodzik & Sanderson, PA	Vachon	Melanson Heath
FY19	$5,250.00	$5,300.00	$8,000.00		$9,525.00	$9,500.00	$11,000.00
FY20	$5,250.00	$5,300.00	$8,250.00		$9,525.00	$9,500.00	$11,350.00
FY21	$5,250.00	$5,300.00	$8,500.00		$9,525.00	$9,500.00	$11,750.00
District 3 Year Total	$15,750.00	$15,900.00	$24,750.00		$28,575.00	$28,500.00	$34,100.00

	Mont Vernon				Souhegan		
	Plodzik & Sanderson, PA	Vachon	Melanson Heath		Plodzik & Sanderson, PA	Vachon	Melanson Heath
FY19	$7,225.00	$7,100.00	$9,000.00		$9,525.00	$9,500.00	$10,000.00
FY20	$7,225.00	$7,100.00	$9,250.00		$9,525.00	$9,500.00	$10,300.00
FY21	$7,225.00	$7,100.00	$9,500.00		$9,525.00	$9,500.00	$10,600.00
District 3 Year Total	$21,675.00	$21,300.00	$27,750.00		$28,575.00	$28,500.00	$30,900.00

SAU 39
AMHERST SCHOOL DISTRICT
MONT VERNON SCHOOL DISTRICT
SOUHEGAN COOPERATIVE SCHOOL DISTRICT

REQUEST FOR PROPOSALS
FINANCIAL AUDITS

The SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District, New Hampshire are seeking proposals and statements of qualification from certified public accounting firms relative to the performance of the SAU and Districts' annual financial audits. Copies of the request for proposals may be obtained from SAU 39, 1 School Street, P.O. Box 849, Amherst, NH 03031. Responses must be received in the SAU Office no later than March 20, 2019 at 3:00 P.M. EST. The SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District reserve the right to accept or reject any or all proposals submitted in response to this request, and also reserve the right to waive any and all formalities.

SAU 39
AMHERST SCHOOL DISTRICT
MONT VERNON SCHOOL DISTRICT
SOUHEGAN COOPERATIVE SCHOOL DISTRICT

REQUEST FOR PROPOSAL
FINANCIAL AUDITS

INTRODUCTION

The SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District invite qualified independent certified public accounting firms to submit proposals for the performance of audits of their general purpose financial statements and related disclosures for the purpose of expressing audit opinions relative to the fairness of the presentations in accordance with accounting principles generally accepted in the United States of America. The auditor(s) shall state that the primary purpose of the audit is to express an opinion on the general purpose financial statements taken as a whole and that the audit is subject to the inherent risk that errors or irregularities may occur and not be detected.

Furthermore, SAU 39 and the School Districts have complied with and intend to maintain compliance with the requirements of Governmental Accounting Standards Board Statement #34.

There is no expressed or implied obligation for the SAU 39, Amherst School District, Mont Vernon School District, or Souhegan Cooperative School District to reimburse firms for any expenses incurred in preparing proposals in response to this request.

To be considered, (3) three copies of a proposal must be received by March 20, 2019, no later than 3:00 P.M. EST at SAU 39, P.O. Box 849, 1 School Street, Amherst, NH 03031. The sealed proposals must be plainly marked "RFP – AUDIT PROPOSAL." SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District reserve the right to reject any or all proposals submitted, and also reserve the right to waive any and all formalities. Submission of a proposal indicates acceptance by the firm of the conditions in this request for proposals, unless clearly and specifically noted in the proposal submitted and confirmed in the agreements between SAU 39, Amherst School District, Mont Vernon School District, and/or Souhegan Cooperative School District and the selected firm.

It is anticipated that the selection of a firm will be completed by April 25, 2019. Following the notification of the selected firm, it is expected that engagement letters will be executed within 30 days of approval.

TERMS OF ENGAGEMENT

A three (3) year contract is contemplated, subject to the annual review and recommendation of the Business Administrator, the satisfactory negotiation of terms, the concurrence of the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District and the annual availability of an appropriation.

The proposals are to cover the following three (3) fiscal years:

(a) July 1, 2018 through June 30, 2019
(b) July 1, 2019 through June 30, 2020

(c) July 1, 2020 through June 30, 2021

QUALIFYING REQUIREMENTS

Firms submitting proposals must be qualified to perform independent audits of school districts of the State of New Hampshire. The auditors must have an office located within the State of New Hampshire, and resident staff must be able to offer the full range of auditing services required by this request for proposals.

Supervisory members of the audit team, including the "in-charge" field auditor, should be Certified Public Accountants and have a minimum of two (2) years of municipal audit experience in the State of New Hampshire. The SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District intend to strongly consider school district audit experience and certification in evaluating the proposer's audit team.

A. GENERAL INFORMATION

The SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District are located in Hillsborough County in the southern part of the state, approximately 15 minutes west of Nashua.

SAU 39 is comprised of approximately 20 employees housed in a building owned by the Amherst School District. Total appropriations for the current year, (FY 2019), are approximately $2.25 million. The most recent audit of the District was conducted in September 2018 for the period July 1, 2017 through June 30, 2018.

The Amherst School District is comprised of almost 1,300 students in grades K-8, two (2) elementary schools and one (1) middle school. Total appropriations for the current year (FY2019) are approximately $28.9 million. The most recent audit of the District was conducted in September 2018 for the period July 1, 2017 through June 30, 2018.

The Mont Vernon School District is comprised of approximately 189 students in grades K-6, approximately 55 students in grades 7 and 8 tuitioned out to Amherst Middle School, and one (1) elementary school. Total appropriations for the current year (FY2019) are approximately $5.2 million. The most recent audit of the District was conducted in September 2018 for the period July 1, 2017 through June 30, 2018.

The Souhegan Cooperative School District is comprised of approximately 740 students from Amherst and Mont Vernon in grades 9-12, and one (1) high school with two (2) buildings. Total appropriations for the current year (FY2019) are approximately $18.2 million. The most recent audit of the District was conducted in September 2018 for the period July 1, 2017 through June 30, 2018.

The accounts of the Districts are organized on the basis of funds, each of which is considered a separate fiscal and accounting entity with a self-balancing set of accounts.

The following types of funds are used by the Districts:

(1) General Funds: to account for all financial resources except those required to be accounted for in another fund.

(2) Special Revenue Funds: to account for the proceeds of specific revenue sources other than expendable trust funds.
(3) Capital Projects Funds for major capital projects that are legally restricted to expenditures for specified purposes.
(4) Trust and Agency Funds: to account for assets held by a governmental unit in a trustee capacity or as an agent for individuals, private organizations, other governmental units, and/or other funds.

The Districts maintain general ledgers for the General Funds, Special Revenue Funds, Capital Projects Funds, and Trust and Agency Funds.

The Districts presently maintain their financial records on a computer system using Infinite Visions software. Payroll, accounts receivable, accounts payable, and general ledgers are maintained as part of a comprehensive budgetary accounting system, along with food services and federal/state/local grants. Government-wide financial statements are prepared using the accrual basis of accounting. At the fund reporting level, governmental funds use the modified accrual basis of accounting.

B. AUDIT STANDARDS

The audit firm shall conduct the audit of the accounts and records of the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District in accordance with generally accepted auditing standards as set forth by the American Institute of Certified Public Accountants, *the standards for financial audits set forth in the U.S. Comptroller General's Government Auditing Standards, the provisions of the Single Audit Act of 1984, the provisions of U.S. Office of Management and Budget (OMB) Circular A-133, and Audits of State and Local Governments*.

C. AUDIT SCOPE

The certified public accounting firm shall be engaged to conduct an audit of the general purpose financial statements, accounts, records, and procedures of all departments and funds of the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District. A Single Audit conducted in accordance with the Single Audit Act of 1984 and OMB Circular A-133, if applicable.

Indicate in your proposal if you agree to meet or exceed the following audit specifications. Explain exceptions you may have regarding any specification.

(1) The firm shall perform a financial audit of all funds reported in the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District financial statements included in the latest Annual Financial Statements Reports which accompany this Request for Proposals.

The audits shall be conducted to satisfy the requirements of the State of New Hampshire Department of Revenue Administration, State of New Hampshire Department of Education, and applicable state and federal laws and regulations.

(2) In connection with the examination of the records and financial statements, the firm shall review the systems of internal controls, operating procedures and compliance with budgetary and legal requirements of the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District.

The reviews of internal controls must include reviews of the related processing controls with respect to data processing operations.

The reviews should also include, but not be limited to, the areas of physical security, systems and program documentation, input/output controls, and control over use and retention of electronic files.

(3) The firm shall perform a financial audit in accordance with the Single Audit Act of 1984 and OMB Circular A-133 for all federally assisted programs, if applicable.

(4) The SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District views their engagement of an audit firm as an ongoing professional relationship in which the firm is expected to provide occasional advisory services, as needed, during the course of each year. As such, the firm is expected to consult as required on auditing, accounting, financial reporting and operating questions, which may arise during the course of the year. In addition, the firm is expected to provide the Districts with information on current developments, which would affect the Districts' financial operations.

(5) The firm shall agree to make available its working papers upon request, to meet any District financial need as well as in accordance with any federal or state grant provision. Working papers will be kept for three (3) years from submission of the final audit report.

(6) The firm shall agree to attend conferences to review the audit program with SAU and School District officials, as well as the local governments' roles and assistance in the audit process.

(7) The partner or manager in charge of the audit shall be available to attend public meetings at which the audit report may be discussed. The partner or manager in charge of the audit shall also be available to discuss the audit report or other reports required by this proposal with the SAU and Districts' financial staff as required.

D. AUDIT AND REPORT SCHEDULES

Indicate in your proposal if you agree to meet the following audit and report schedules. Explain exceptions you may have regarding any of the requirements.

(1) The firm shall conduct the audits covering operations of the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District and of federally assisted programs (if any) during the following periods:

(a) July 1, 2018 through June 30, 2019
(b) July 1, 2019 through June 30, 2020
(c) July 1, 2020 through June 30, 2021

The firm shall submit Independent Auditor's Reports containing expressions of opinion that the general purpose financial statements are fairly stated, or, if a qualified or adverse opinion or disclaimer of opinion is necessary, the reasons therefore. The firm shall submit six (6) bound and one (1) electronic copy of its SAU report, six (6) bound and one (1) electronic copy of its Amherst School District report, six (6) bound and one (1) electronic copy of its Mont Vernon report, and eight (8)

bound and one (1) electronic copy of its Souhegan Cooperative report no later than November 30th of each year.

(2) The firm shall submit a written report on the internal control structure, which shall identify reportable conditions and/or material weaknesses, assess their effects and propose initial steps to mitigate them. The firm shall submit the same number of bound copies of the final draft of the report on the internal control structure and memorandum of comments and recommendations, which identifies observed operational conditions and/or practices no later than November 30th of each year.

(3) The SAU and the School Districts reserve the right to request additional auditing services to be performed in conjunction with the annual financial audit. If such services are requested by a District and/or the SAU and agreed to by the firm, the firm shall provide a written quotation on the additional cost of said services, if any. During the course of performing such additional service, the firm agrees that it will notify the District and/or SAU, in writing, if unanticipated work arises which would cause an increase in service fees. If additional costs are incurred by the firm and the District and/or the SAU has not agreed to such additional costs, the District and/or the SAU shall have no obligation to pay the additional costs.

(4) The firm shall also be responsible for answering inquiries from the Business Administrator and/or Business Office throughout the year for each of the years covered by the contract. The Firm shall meet and/or confer no less than once per year (outside the audit) with representatives of the Business Office to review and discuss changes in laws, rules, regulations and suggested practices that would affect the operation of the Business Office.

E. TECHNICAL PROPOSAL

(1) General Requirements

The purpose of the technical proposal is to demonstrate the qualifications, competence, and capacity of the firms seeking to undertake an independent audit of the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District in conformity with the requirements of this request for proposals. As such, the substance of proposals will carry more weight than their form or manner of presentation. The technical proposal should demonstrate the qualifications of the firm and of the particular staff to be assigned to this engagement. It should also specify an audit approach that will meet the request for proposals requirements.

The technical proposal should address all the points outlined in the request for proposals (excluding any cost information which should only be included in schedules provided with this request). The proposals should be prepared simply and economically, providing a straightforward, concise description of the firm's capabilities to satisfy the requirements. While additional items may be presented, the following subjects must be included. They represent the criteria against which the proposal will be evaluated.

(2) Independence

The firm should provide an affirmative statement that it is independent of the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District as defined by generally accepted accounting standards and the U.S. Comptroller General's Government Auditing Standards.

The firm should also list and describe the firm's professional relationships involving the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District or any of its agencies for the past five (5) years, together with a statement explaining why such relationships do not constitute a conflict of interest relative to performing the proposed audit.

In addition, the firm shall give the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District written notice of any professional relationships entered into during the period of this agreement.

(3) License to Practice in New Hampshire

An affirmative statement should be included indicating that the firm and its municipal partner are qualified to practice in New Hampshire.

(4) Firm Qualifications and Experience

The proposal should state the size of the firm, the size of the firm's governmental audit staff, the location of the office from which the work on this engagement is to be performed and the number and nature of the staff to be so employed on a part-time basis.

The firm shall also provide information on the results of the firm's latest federal or state desk reviews or field reviews of its audits. In addition, the firm shall provide information on the circumstances and status of any disciplinary action taken or pending against the firm during the past three (3) years with state regulatory bodies or professional organizations.

(5) Partner, Supervisory and Staff Qualifications and Experience

The firm should identify the principal supervisory and management staff, including engagement partners, managers, other supervisors and specialists, who would be assigned to the engagement and indicate whether each such person is licensed to practice as a Certified Public Accountant in New Hampshire. The firm also should indicate how the quality of staff over the term of the agreement will be assured.

Engagement partners, managers, other supervisory staff and specialists may be changed if those personnel leave the firm, are promoted, or are assigned to another office. These personnel may also be changed for other reasons with prior written agreement of SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District. However, in either case, the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District retain the right to approve or reject replacements.

Consultants and firm specialists mentioned in response to this request for proposals can only be changed with prior written agreement of the SAU 39, Amherst School District, Mont

Vernon School District, and Souhegan Cooperative School District, which retains the right to approve or reject replacements.

Other audit personnel may be changed at the discretion of the proposer provided that replacements have substantially the same or better qualifications or experience.

(6) Similar Engagements with Other Government Entities

For the firm's office that will be assigned responsibility for the audit, list the most significant engagements (maximum of 5) performed in the last five (5) years that are similar to the engagement described in this request for proposals. These engagements should be ranked on the basis of total staff hours. Indicate the scope of work, date, engagement partners, total hours, and the name and telephone number of the principal client contact.

(7) Audit Approach

The proposal should set forth a work plan, including an explanation of the audit methodology to be followed, to perform the services required in this request for proposal. In developing the work plan, reference should be made to such sources of information as the Districts' budgets and related materials, organizational charts, manuals and programs, and financial and other management information systems.

(8) Identification of Anticipated Potential Audit Problems

The proposal should identify and describe any anticipated potential audit problems, the firm's approach to resolving these problems, and any special assistance that will be requested from the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District.

F. EVALUATION PROCEDURES

The SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District shall evaluate the proposals on the basis of the qualifications, relevant experience and responsiveness of the bidders, as well as the staffing and estimated cost of the engagement. The District may wish to conduct oral interviews with the firms considered most qualified in order to help the District in the selection process.

G. ASSISTANCE BY THE DISTRICT

The SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District's financial staff shall render all feasible assistance to the audit firm and shall respond promptly to requests for information, provide all necessary books and records, and provide physical facilities required by the firm for the expeditious conduct of the engagement. It is anticipated that the books and records for the Districts will be closed and ready for audit by August 31st of each year. The fieldwork for the successful bidder should be scheduled as soon as possible thereafter with a completion date no later than September 30th of each year.

H. COMPENSATION

The firm's proposal must indicate the maximum total your firm will charge the District for each year of this proposal. The maximum fee must be broken down as indicated on the attached fee schedule for each year.

The final payment for any audit shall become due only after submission of all reports required by this document and their acceptance by the SAU and the Districts and/or federal and state grantor agencies.

Should the firm encounter circumstances requiring an increase in the extent of detailed investigation, or should the SAU and/or the Districts require an increase in the scope of the audit, written notice to that effect must be given to the other party.

The engagement may then be modified by mutual agreement as to additional work end compensation.

I. TERMINATION OF THE AUDIT

If the audit firm fails to substantially comply with the specifications set herein, the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District reserve the right to terminate the engagement after completion of any audit year upon written notice to the firm.

J. INSURANCE

The professional individual or firm shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from, or be in connection with the performance of the work hereunder by the individual or the firm, his agents, representatives, or employees.

For the purpose of this clause, the term "professional individual or firm" shall also include the individual's or firm's respective officers, agents, officials, employees, volunteers, boards, and commissions.

K. SUBMITTAL INFORMATION

Proposals, including completed copies of the attached Proposer Guarantees and Warranties on page 10 as well as the attached fee schedules for the SAU and each District beginning on page 11, must be marked "RFP - AUDIT PROPOSAL" and received no later than March 20, 2019 at 3:00 P.M EST. All technical services information must be enclosed in an envelope marked "technical specifications" and all pricing schedules submitted in an envelope marked "pricing schedules". All submittals shall be addressed to SAU 39, PO Box 849, 1 School Street, Amherst, NH 03031. Any inquiries should be directed to Katie Hannan, Director of Finance, via email at khannan@sprise.com.

PROPOSER GUARANTEES AND WARRANTIES

Proposer Guarantees

The proposer certifies that it can and will provide and make available, at a minimum, all services set forth in this request for proposals.

Proposer Warranties

1. The proposer warrants that it is willing and able to obtain an errors and omissions insurance policy providing a prudent amount of coverage for the willful or negligent acts, or omissions of any officers, employees or agents thereof.

2. The proposer warrants that it will not delegate or subcontract its responsibilities under an agreement without the express prior written permission of the SAU 39, Amherst School District, Mont Vernon School District, and Souhegan Cooperative School District.

3. The proposer warrants that all information provided by it in connection with this proposal is true and accurate.

Signature of Official: _____

Name (typed): _____

Title: _____

Firm: _____

Date: _____

SAU 39
Summary Schedule of Professional Fees and Expenses
For the Audit of Financial Statements

	FY2019	**FY2020**	**FY2021**	**Total**
Standard Audit				
Total				

The undersigned proposes to provide the SAU 39 with an independent audit of its financial accounts and records, as outlined in the accompanying specifications and that I will accept as full payment thereof, the sums indicated on this schedule.

Signature of Official: _____

Name (typed): _____

Title: _____

Firm: _____

Date: _____

Amherst School District
Summary Schedule of Professional Fees and Expenses
For the Audit of Financial Statements

	FY2019	**FY2020**	**FY2021**	**Total**
Standard Audit				
A-133 Single Audit, (if required)				
Total				

The undersigned proposes to provide the Amherst School District with an independent audit of its financial accounts and records, as outlined in the accompanying specifications and that I will accept as full payment thereof, the sums indicated on this schedule.

Signature of Official: _____

Name (typed): _____

Title: _____

Firm: _____

Date: _____

Mont Vernon School District
Summary Schedule of Professional Fees and Expenses
For the Audit of Financial Statements

	FY2019	**FY2020**	**FY2021**	**Total**
Standard Audit				
A-133 Single Audit, (if required)				
Total				

The undersigned proposes to provide the Mont Vernon School District with an independent audit of its financial accounts and records, as outlined in the accompanying specifications and that I will accept as full payment thereof, the sums indicated on this schedule.

Signature of Official: _____

Name (typed): _____

Title: _____

Firm: _____

Date: _____

Souhegan Cooperative School District
Summary Schedule of Professional Fees and Expenses
For the Audit of Financial Statements

	FY2019	**FY2020**	**FY2021**	**Total**
Standard Audit				
A-133 Single Audit, (if required)				
Total				

The undersigned proposes to provide the Souhegan Cooperative School District with an independent audit of its financial accounts and records, as outlined in the accompanying specifications and that I will accept as full payment thereof, the sums indicated on this schedule.

Signature of Official: _____

Name (typed): _____

Title: _____

Firm: _____

Date: _____

Insights Report

School Administrative Unit 39

Fall 2017 to Fall 2018

Executive Summary: Achievement and Growth

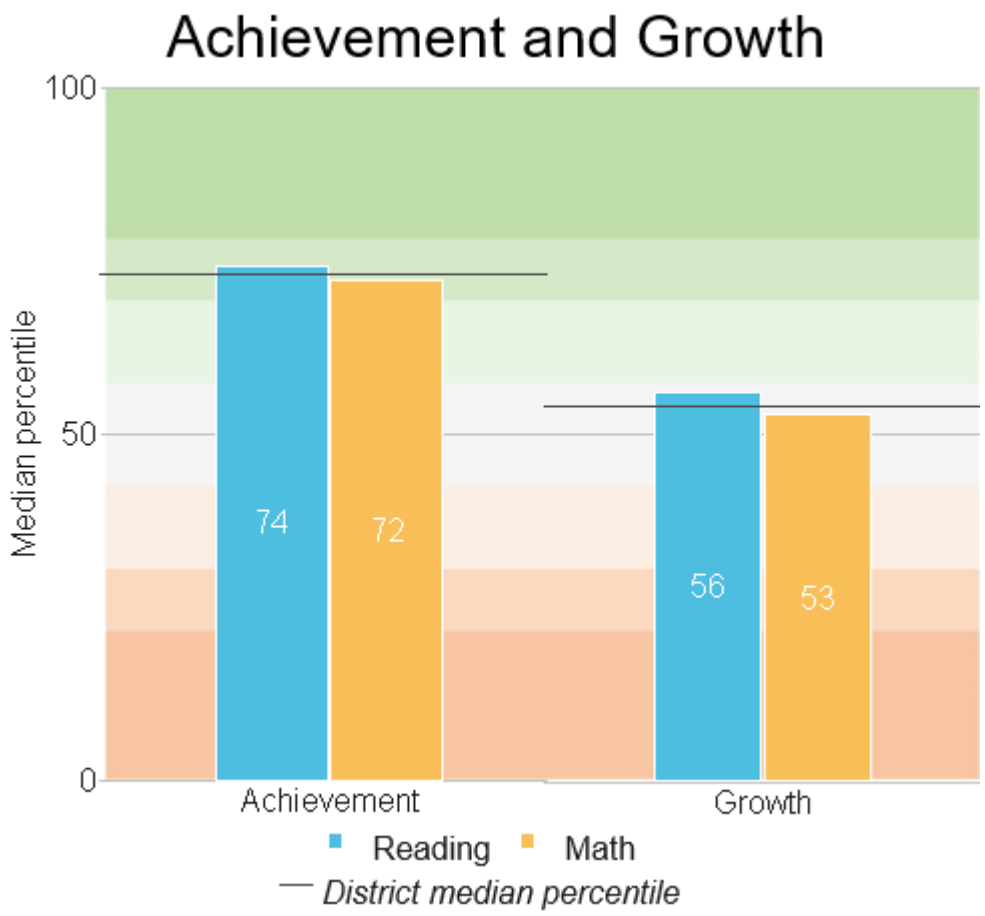
Achievement is moderately above average while growth is average.

District median achievement is 73rd percentile.

Reading was above median.
Mathematics was below median.

District median growth is 54th percentile.

Reading was above median.
Mathematics was below median.



Executive Summary: Proficiency and College Readiness

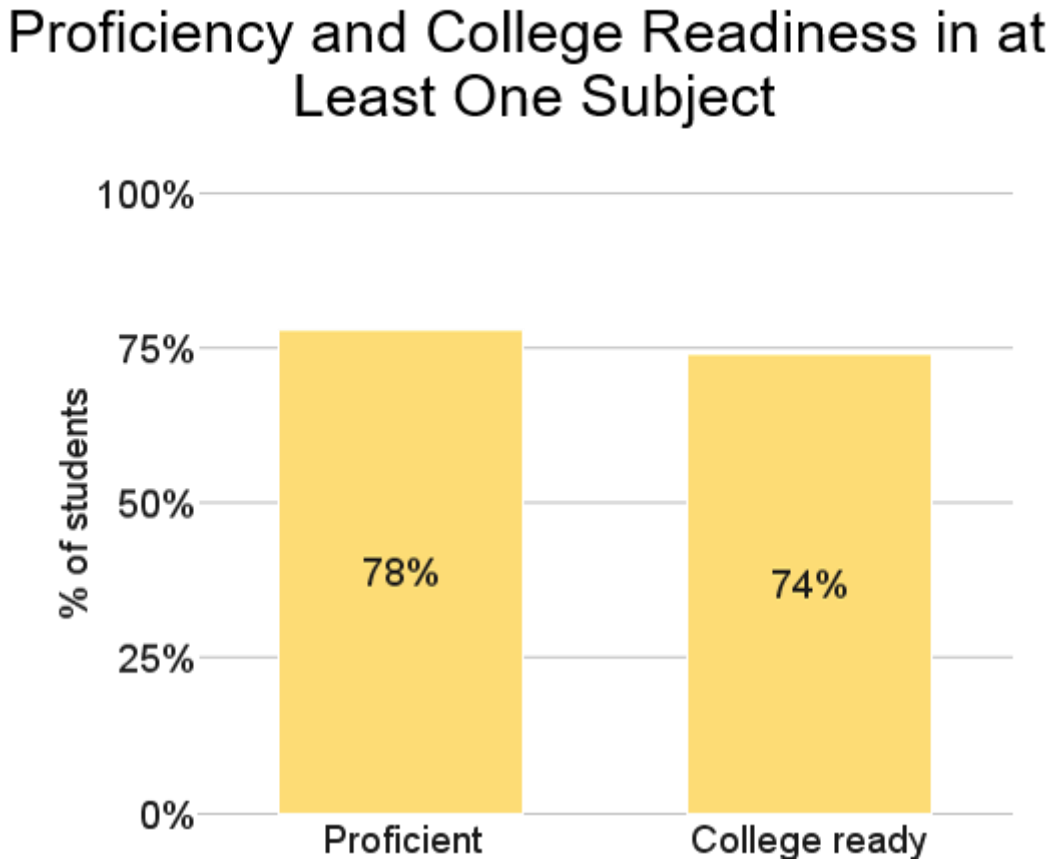
In at least one subject, 78% of students should meet state standards and 74% are on track for college readiness.

Projected proficiency: ELA is higher

72% proficient in ELA
55% proficient in math
78% proficient in ELA or math

College readiness: ELA is higher

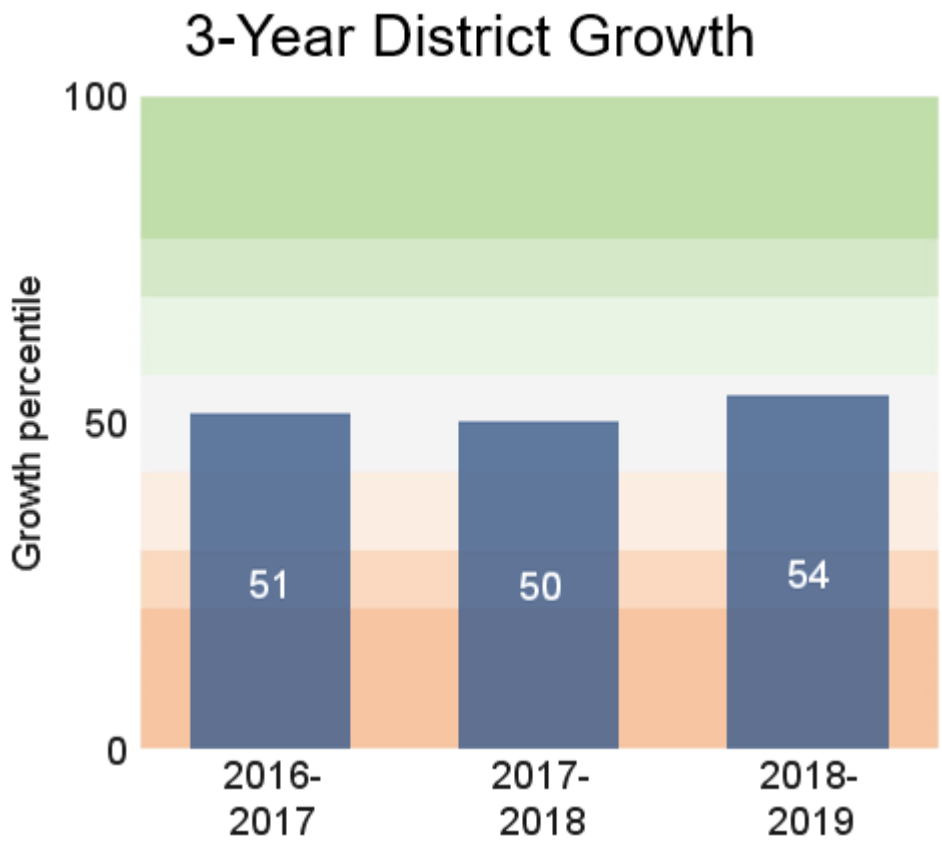
68% college ready in ELA
54% college ready in math
74% college ready in ELA or math



Executive Summary: Longitudinal Growth

The district's 3-year growth has been consistently average.

2016-17 growth percentile is average (51)
2017-18 growth percentile is average (50)
2018-19 growth percentile is average (54)



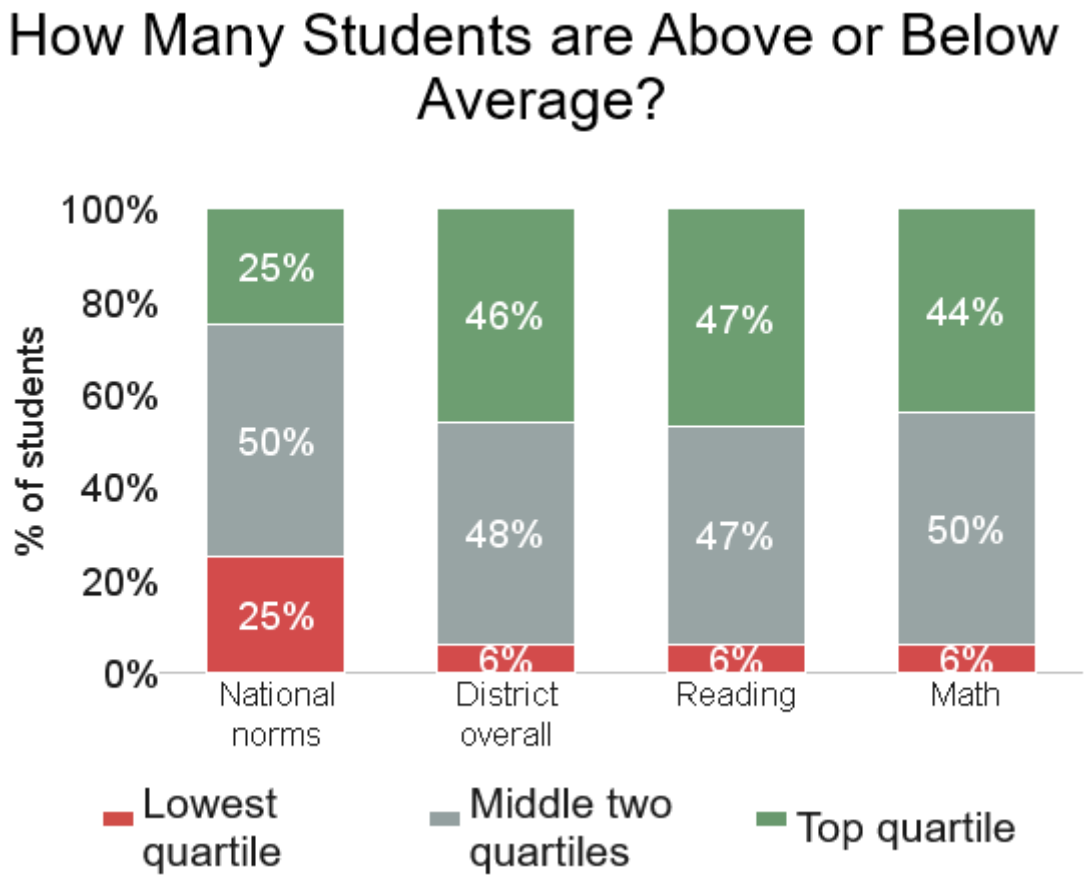
How are District Students Doing: Achievement Status

Fall 2017 achievement scores show a larger proportion of students in the top quartile than national norms.

Top quartile: a larger proportion (46%) than is typical (25%)

Middle two quartiles: a typical proportion (48%) when compared to national norms (50%)

Lowest quartile: a smaller proportion (6%) than is typical (25%)



How are District Students Doing: Growth by Quartile

Lowest-quartile students grew substantially faster than top-three-quartiles students from fall to fall.

Top quartile: growth (49th) approximately equal to the norm

Middle two quartiles: growth (57th) approximately equal to the norm

Lowest quartile: substantially more growth (83rd) than the norm

Are Students Growing Equally?

	Lowest quartile	Middle two quartiles	Top quartile
Reading	86th	59th	49th
Math	81st	54th	48th
Total	83rd	57th	49th
Norm	50th	50th	50th

How are District Students Doing: by Decile

Overall growth of top decile students is average, while bottom decile students is substantially above the norm.

Top decile: a larger proportion (19%) than is typical (10%)
Growth percentile: 46th

Bottom decile: a smaller proportion (2%) than is typical (10%)
Growth percentile: 92nd

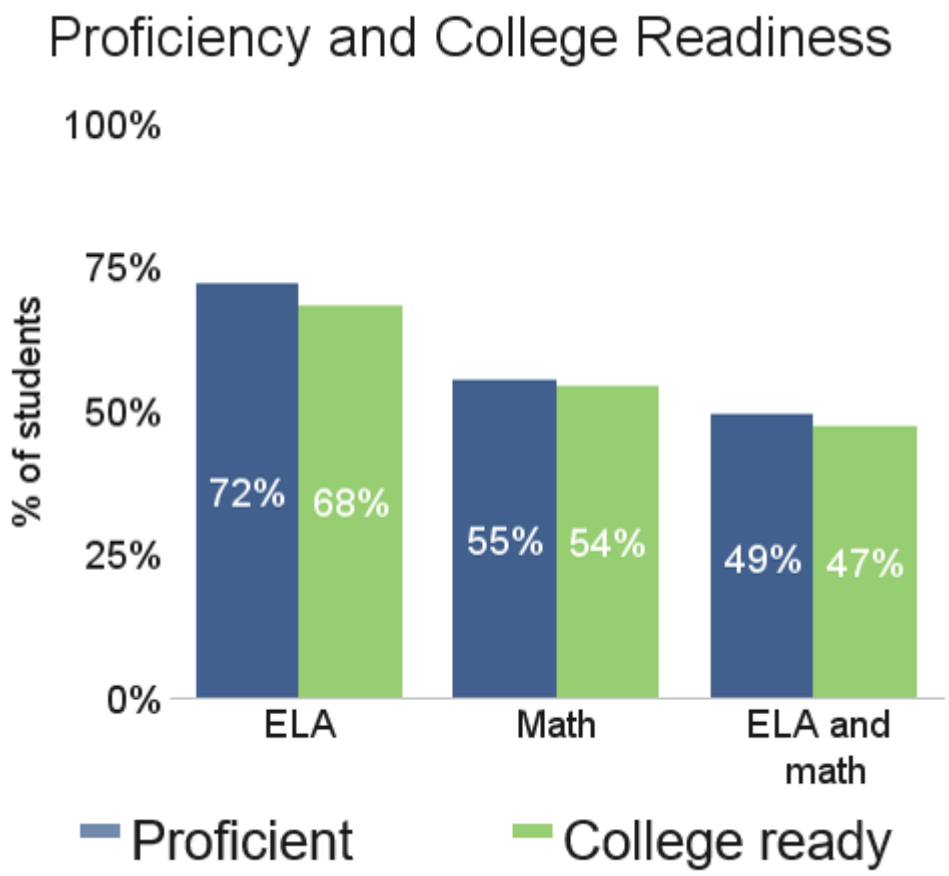
Are Students Growing Equally?

	Bottom decile	Top decile
Total	92nd	46th
Norm	50th	50th

Are We Proficient & College Ready: Overview

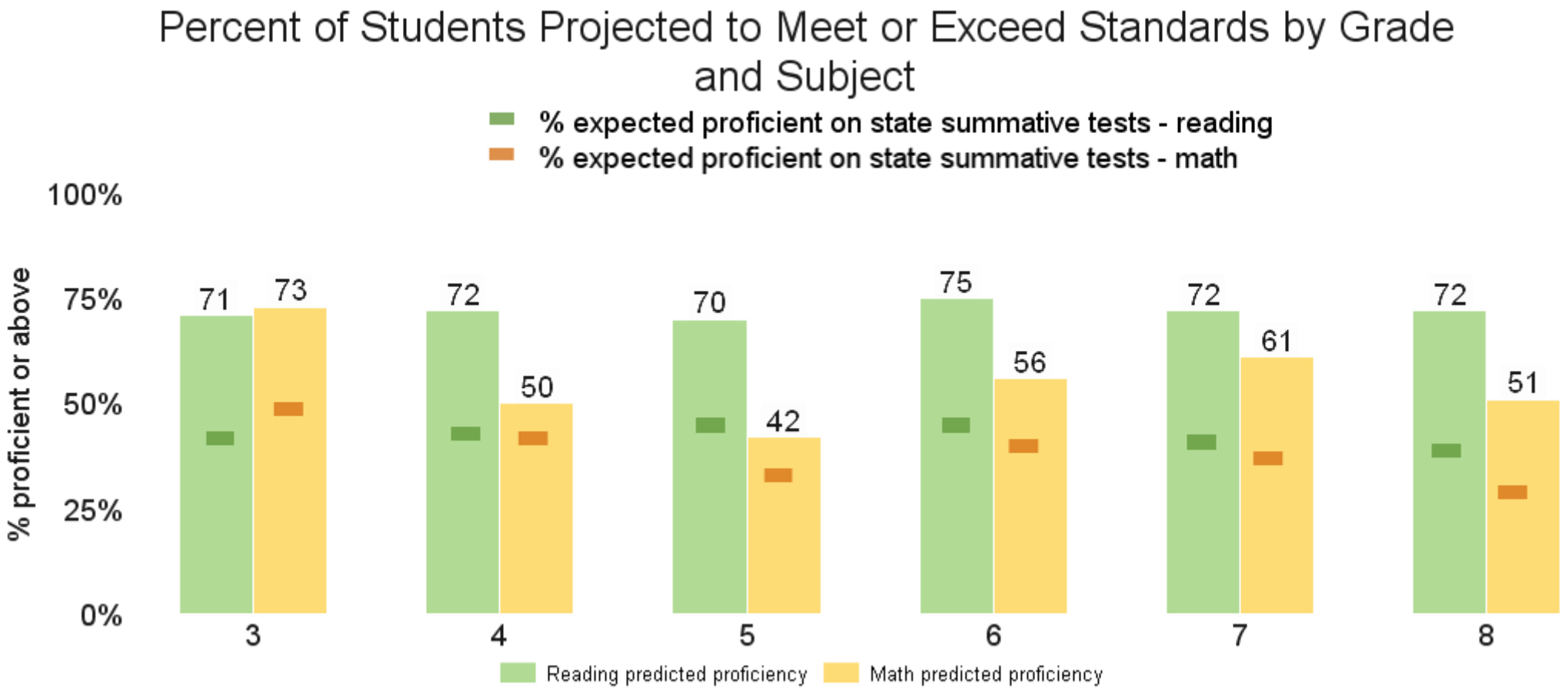
In both ELA and math, 49% of students should meet state standards and 47% are on track for college readiness.

	Proficiency rate	College readiness rate
ELA only	72%	68%
Math only	55%	54%
Both ELA and math	49%	47%
Neither ELA or math	22%	26%



Are We Proficient & College Ready: Proficiency by Grade and Subject

Proficiency rates are above national benchmarks for all tested grades with norms in both reading and math.

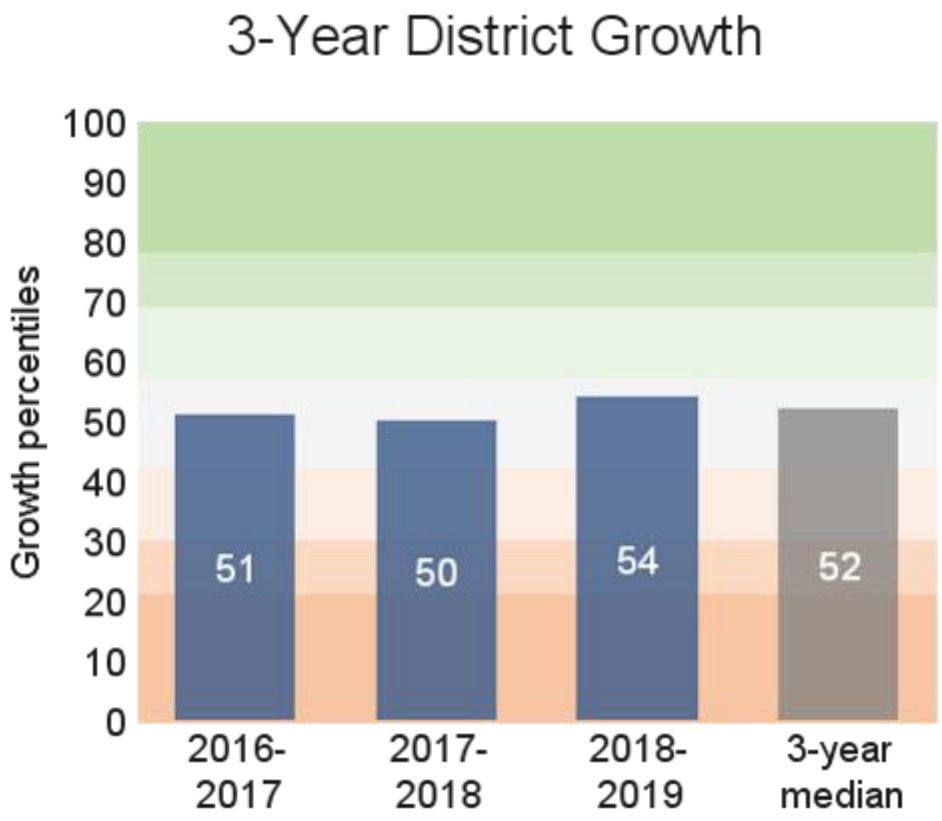


Is Our Growth Strong Over Time?

3-year growth is average relative to national norms; reading and math are consistently average.

3-Year Growth Percentile by Subject

	2016-17	2017-18	2018-19	Total
Reading	50	47	56	51
Math	53	53	53	53
Total	51	50	54	52



How is Status by Grade & Subject?

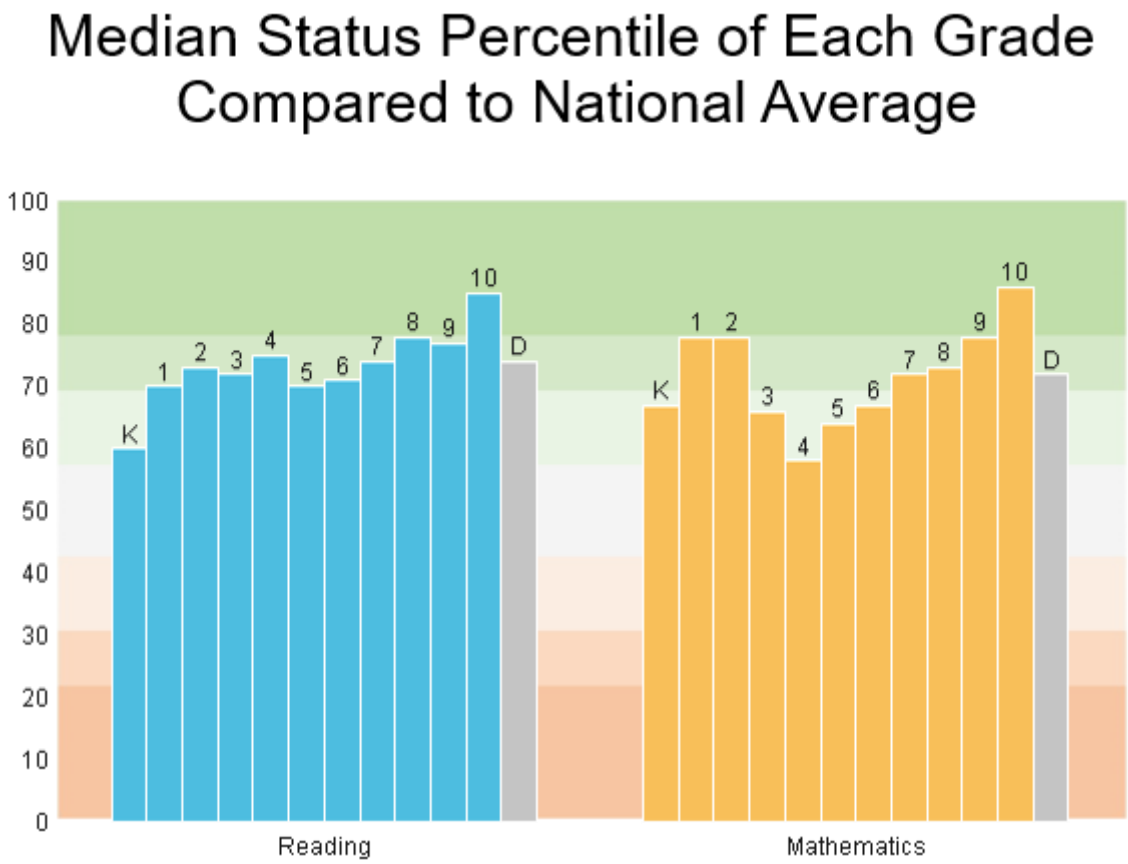
All grades had above average status in both subjects.

Reading had the highest achievement overall.

Ranged from 60th percentile for K to 85th percentile for 10th grade

Mathematics had the lowest achievement overall.

Ranged from 58th percentile for 4th grade to 86th percentile for 10th grade



How is Growth by Grade & Subject?

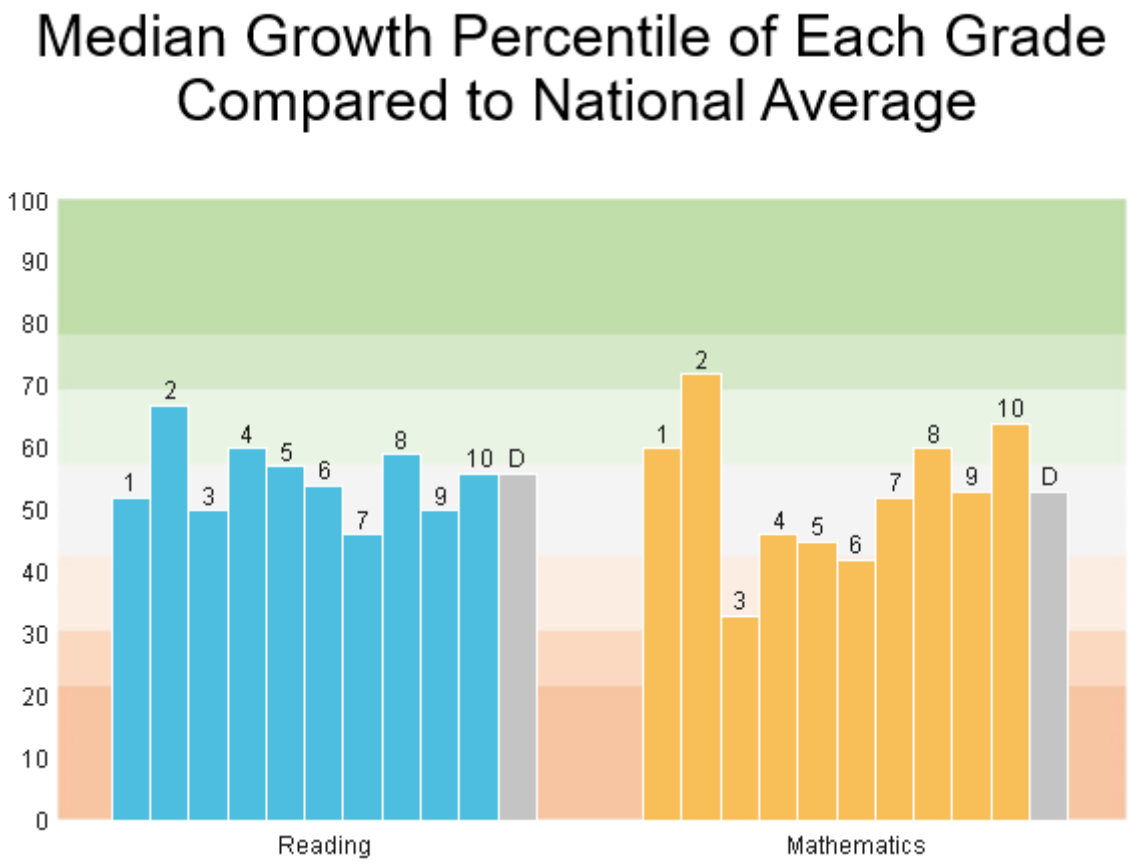
2nd and 8th grades had above average growth in both subjects; 3rd and 6th grades had below average growth in one subject.

Reading had the highest growth overall.

Ranged from 46th percentile for 7th grade to 67th percentile for 2nd grade

Mathematics had the lowest growth overall.

Ranged from 33rd percentile for 3rd grade to 72nd percentile for 2nd grade

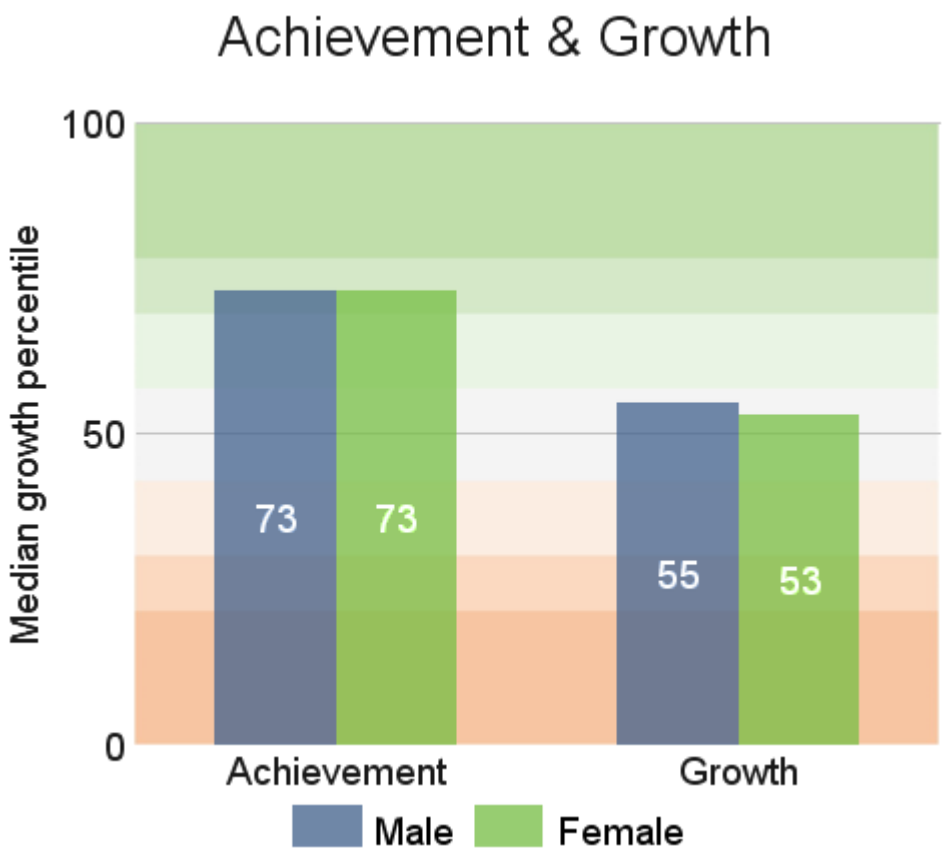


How Do Boys and Girls Compare: Overview

Both median achievement and growth were about the same for girls and boys, respectively.

Girls and boys both had moderately above average achievement.

Girls and boys both had average growth.



How Do Boys and Girls Compare: by Subject and Grade Span

There is no significant difference between girls and boys across all grade spans and all subjects.

In grades K–5:

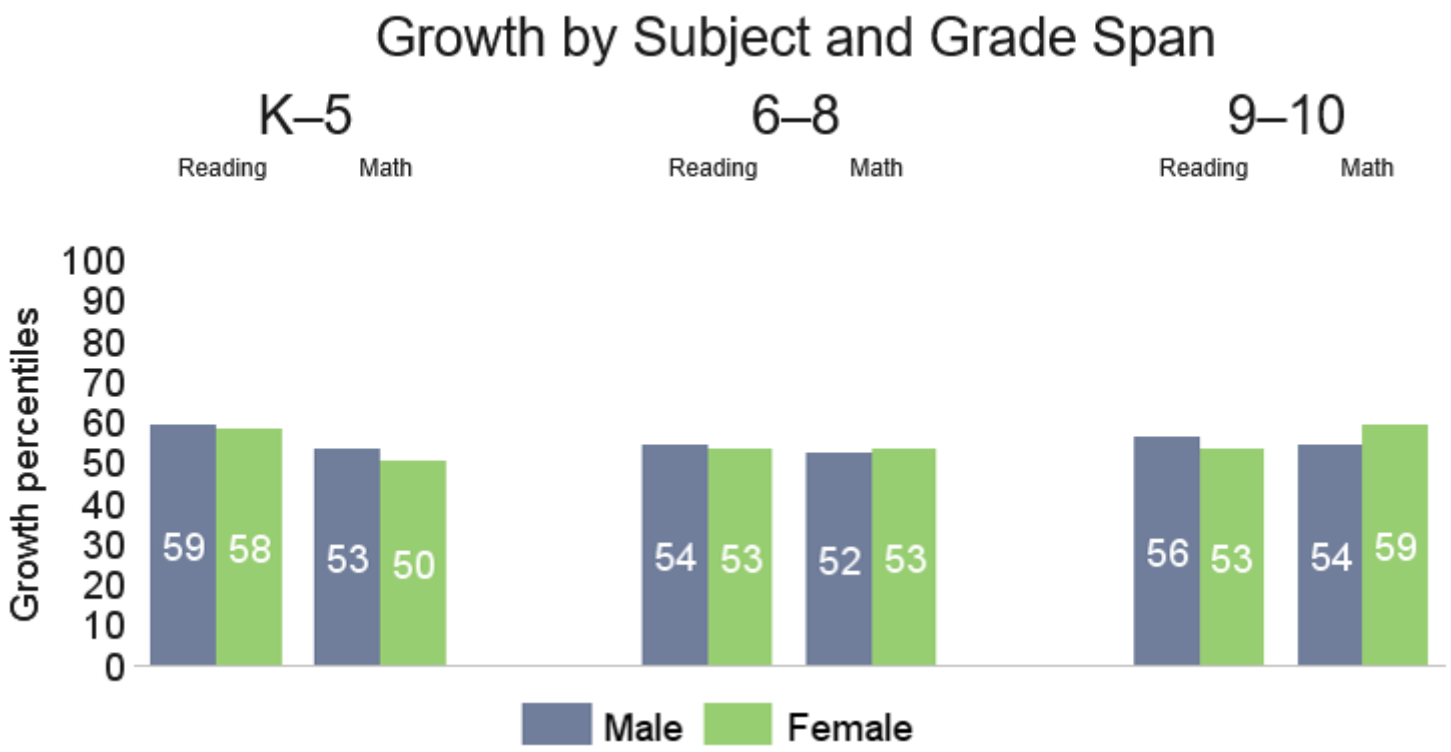
girls and boys had relatively the same growth in reading and math.

In grades 6–8:

girls and boys had relatively the same growth in reading and math.

In grades 9–10:

girls and boys had relatively the same growth in reading and math.



School Administrative Unit 39

Data Security and Data Privacy Guidelines

May, 2019

DRAFT

Contents

Introduction
- Data Governance Team
- Purpose
- Scope
- Regulatory Compliance
- Data User Compliance

Data Lifecycle
- Identifying Need & Assessing Systems for SAU Requirements
  - New Systems
  - Review of Existing Systems
- Acquisition and Creation
- Management and Storage
  - Systems Security
  - Data Management
  - Data Classification and Inventory
- Security/Protection
  - Risk Management
  - Security Logs
  - Physical Security Controls
  - Inventory Management
  - Virus, Malware, Spyware, Phishing and SPAM Protection
  - Electronic Access Security Controls
  - Securing Data at Rest and Transit
- Usage and Dissemination
  - Data Storage and Transmission
  - Training
- Archival and Destruction
  - Data Destruction Processes
  - Asset Disposal

Critical Incident Response
- Business Continuity
- Disaster Recovery
- Data Breach Response

Appendix A - Definitions

Appendix B - Laws, Statutory, and Regulatory Security Requirements

Appendix C - Digital Resource Acquisition and Use

Appendix D - Data Security Checklist

Appendix E - Data Classification Levels

Appendix F - Securing Data at Rest and Transit

Appendix G - Physical Security Controls

Appendix H - Asset Management

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

Appendix J - Account Management

Appendix K - Data Access Roles and Permissions

Appendix L - Password Security

Appendix M - Technology Disaster Recovery Plan

Appendix N - Data Breach Response Plan

Introduction

School Administrative Unit 39 ("SAU 39" and "the SAU" will be used throughout this document to represent the four units of School Administrative Unit 39 – the Amherst School District, the Mont Vernon School District, the Souhegan Cooperative School District and School Administrative Unit 39) 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.

The SAU 39 Data Security and Privacy Guidelines includes information regarding the data governance team, data and information governance, applicable School Board policies, SAU procedures, as well as applicable appendices and referenced supplemental resources.

This document outlines how operational and instructional activity shall be carried out to ensure the SAU 39 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.

The SAU 39 Data Security and Privacy Guidelines 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 SAU 39 website.

Data Governance Team

The SAU 39 Data Governance team consists of the following positions: Superintendent, Assistant Superintendent, Business Administrator, Director of Buildings and Grounds, Director of Human Resources, Director of Student Services and the Director of Technology. Members of the Data Governance Team will act as data stewards for all data under their direction. The Director of Technology will act as the Information Security Officer (ISO), with assistance from members of the full Technology team. The Lead Network Administrator is the SAU's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available. All members of the SAU administrative team will serve in an advisory capacity as needed.

Purpose

The School Boards recognize the value and importance of a wide range of technologies for a well-rounded education, enhancing the educational opportunities and achievement of students. SAU 39 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 SAU 39.

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

It is the policy of the SAU 39 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 SAU contractors or agents using confidential information will strictly observe protections put into place by the SAU.

Scope

The data security policy, standards, processes, and procedures apply to all students and staff of SAU 39, contractual third parties and agents of the SAU, and volunteers who have access to SAU data systems or data. This policy applies to all forms of SAU 39 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 document, 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 SAU 39 and shall be protected from misuse, unauthorized manipulation, and destruction.

Regulatory Compliance

SAU 39 will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix B: Laws, Statutory, and Regulatory Security Requirements). SAU 39 will comply with or exceed the https://www.education.nh.gov/data/documents/minimum-standards-privacy.pdf approved in 2019 and standards applicable to data governance are addressed throughout this Data Security and Privacy Guidelines. SAU 39 will be in compliance 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 and Section 504 of the Rehabilitation 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 Security and Data Privacy Guidelines apply to all users of SAU 39 information including: staff, students, volunteers, and authorized SAU contractors or agents. All data users are to maintain compliance

with School Board Policies and SAU administrative procedures, EHAB (Data Governance and Security), EGA (School District Internet Access for Students), EHAA (Computer Security, Email and the Internet) and all policies, procedures, and resources as outlined within this document and School Board Policy.

A consistently high level of personal responsibility is expected of all users granted access to the SAU's technology resources. Any violation of SAU 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 SAU 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 SAU's premises or the SAU's network, remove a device containing confidential or critical data from the SAU's premises, or modify or copy confidential or critical data for use outside the SAU. If permission is given, the data may be accessed only on a SAU-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 SAU policies or procedures regarding data governance and security may be disciplined or terminated. Volunteers may be excluded from providing services to the SAU. The SAU will end business relationships with any contractor who fails to follow the law, SAU policies or procedures, or the confidentiality provisions of any contract. In addition, the SAU 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 SAU may suspend all access to data or use of SAU technology resources pending an investigation. Violations may result in temporary, long-term or permanent suspension of user privileges. The SAU 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 SAU.

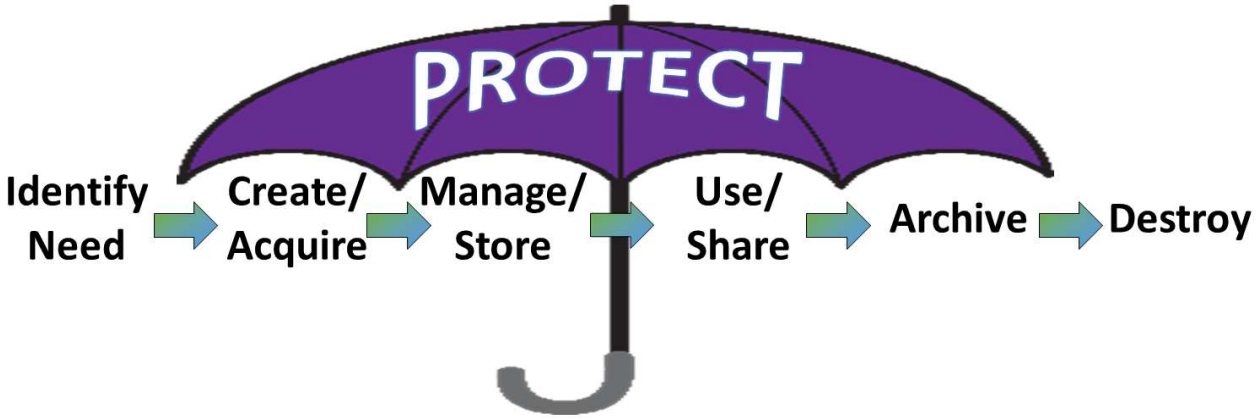
Any attempted violation of SAU policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

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 SAU technological systems.
- The intentional unauthorized altering, destruction, or disposal of SAU information, data and/or systems. This includes the unauthorized removal of technological systems such as but not limited to the following: laptops, internal or external storage, computers, 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 SAU Requirements

To accomplish the SAU 39 mission and to comply with the law, the SAU may need to maintain confidential information, including information regarding students, parents/guardians, staff, applicants for employment and others. The SAU will collect, create or store confidential information only when the Superintendent or designee determines it is necessary.

New Systems

SAU 39 staff members are encouraged to research and utilize online services or applications to engage students and further the SAU'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(s) must approve the use of the service or application and verify that it meets the requirements of the law and School Board policies and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

SAU 39 has an established process for vetting new digital resources. Staff are required to complete steps outlined at the Technology section of the SAU 39 website, to ensure that all new resources meet mission 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 ISO prior to initiation.

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

- Impact on the 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
- Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
  - SAU 39 continues to own the data shared, and all data must be available to the SAU upon request.
  - SAU 39 vendor's access to and use of SAU 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 SAU. If metadata is collected, it will be protected to the same extent as the SAU's confidential or critical information.
  - SAU data will be maintained in a secure manner by applying appropriate technical, physical

and administrative safeguards to protect the data.
- The provider will comply with SAU guidelines for data transfer or destruction when contractual agreement is terminated.
- No API will be implemented without full consent of the SAU.
- All data will be treated in accordance to federal, state and local regulations
- The provider assumes liability and provides appropriate notification in the event of a data breach.

Note: Exceptions can be made by the ISO 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 SAU vetted and approved applications and tools.

A current list of all vetted and approved software systems, tools and applications is available through the links on the Technology section of the SAU 39 Technology website.

Review of Existing Systems

SAU 39 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 SAU 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 SAU will audit data imports annually. These audits should include:

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

Acquisition and Creation

After reviewing the requirements for adoption of any new systems, staff shall complete an online request form for any new digital app/tool that either has an associated cost or collects staff or student data (see Appendix C: Digital Resource Acquisition and Use). 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 ISO 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 creating 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 SAU mission 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 for security/privacy by the Director of Technology, or designee, prior to adoption.

Systems Security

SAU 39 will provide access to confidential information to appropriately trained SAU staff and volunteers only when the SAU determines that such access is necessary for the performance of their duties. The SAU will disclose confidential information only to authorized SAU contractors or agents who need access to the information to provide services to the SAU and who agree not to disclose the information to any other party except as allowed by law and authorized by the SAU (School Board Policy EHAB). Therefore, systems access will only be given on an as-needed basis as determined by the data manager and ISO. Further information regarding Electronic Access Security Controls is contained in the Security/Protection section of this document.

Data Management

The effective education of students and management of SAU personnel often require the SAU to collect information, some of which is considered confidential by law and SAU policy. In addition, the SAU maintain information that is critical to SAU operations and that must be accurately and securely maintained to avoid disruption to SAU 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 SAU administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage. 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 SAU processes to ensure that data will be tracked accurately.
- Review contracts with instructional and operational software providers to ensure that they are current and meet the SAU 39 data security guidelines.
- Ensure that staff are trained in the SAU's proper procedures and practices in order to ensure accuracy and security of data.
- Assist the ISO in enforcing SAU 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 (i.e. source document, electronic record, report) have the same classification regardless of format (see Appendix E: Data Classification Levels).

The ISO or designee will identify all systems containing SAU data, such as student information systems, financial systems, payroll systems, transportation systems, food-service systems, email systems, instructional software applications and others.

The SAU 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
- Staff or staff categories that have access to the files
- Criticality/Sensitivity Rating

Security/Protection

Risk Management

A thorough risk analysis of all SAU 39 data networks, systems, policies, and procedures shall be conducted on a bi-annual basis by an external third party or as requested by the Superintendent, ISO or designee. An internal audit of SAU network security will be conducted annually by SAU 39 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 SAU 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 Director of Technology, Network Administrator and or Director of Facilities. 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 SAU shall maintain a process for inventory control in accordance to federal and state requirements and School Board policy. All SAU 39 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 SAU 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 SAU protection systems or install other systems (see Appendix I: Virus, Malware, Spyware, Phishing and SPAM Protection).

Electronic Access Security Controls

SAU staff will only access personally identifiable and/or confidential information if necessary, to perform their duties. The SAU will only disclose this information to authorized SAU contractors or agents who need access to the information to provide services to the SAU 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 SAU policies 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 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 user access to an application/software is no longer necessary.

Staff Users

All new staff accounts are authorized through a Human Resources 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 ISO 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 and the ISO. All contractors doing business on SAU premises must also pass a background check unless other security measures are addressed in a vendor contract. Contractor/vendor will be granted access to data as needed and approved by the ISO or designee. Once the approval has been obtained, the technology department will create the account providing or access to the application/information that the contractor/vendor supports.

Password Security

The SAU will enforce secure passwords for all systems within their control (see Appendix L: Password Security). When possible, the SAU will utilize Single Sign On (SSO) or LDAP/Active Directory Integration to maintain optimal account security controls.

Concurrent Sessions

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

Remote Access

Access into the SAU's network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the SAU's network and systems; no other method of remote access shall be granted without explicit authorization from the ISO. 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 SAU 39 network.

If a secured connection is needed by a contractor/vendor, access must be approved by the ISO. The Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

All non-SAU 39 accounts will be reviewed at least annually to determine if remote access is needed.

Securing Data at Rest and Transit

SAU data security applies to all forms of data, including data stored on devices, data in transit and data stored on additional resources. Regular transmission of student data to internal and external services is managed by the technology department using 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 SAU technology resources. All SAU 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 SAU 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, Data Governance and Security (EHAB), and Student Records.

SAU staff, contractors and agents will notify the ISO 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 SAU owned device will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students may not be able to store data on the local device. It is important to note that this data is not a part of the SAU storage plan, and thus may not be backed up by the SAU backup solution. Staff and students will also have a mapped personal folder. This folder acts as a redirection of document folders to SAU file servers or cloud storage. Access to these files is restricted to the folder's owner (staff or student who is assigned) and SAU enterprise administrator accounts. Staff and students using devices which have limited local storage capabilities are to store data within their Office 365 OneDrive account or their G Suite for Education 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 an Office 365 OneDrive account and a G Suite for Education account. which provide significant storage. Users are responsible for all digital content on their SAU provided account Drives (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 that contain PII through email or third-party file transfer services without SAU approval. When possible, staff should de-identify or redact any PII or confidential information prior to transmission. Regular transmission of student data to services such as a single sign on provider is managed by the technology group 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 ISO 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 SAU shall create and maintain a data security training program. This program will consist of the following:

- Training for all staff on technology policies and procedures, including confidentiality and data privacy.
- Additional training for new instructional staff on federal regulations and the use of digital resources and student electronic records.
- Training for all instructional staff on federal regulations and the use of digital resources and student electronic records.
- Training for SAU 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 ISO 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 irretrievable.

SAU 39 Data Destruction Processes

The SAU will regularly review all existing data stored on SAU 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. SAU 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 Office 365 and G Suite for Education accounts will be maintained for one school year after the student's final date of attendance.
- Staff G Suite for Education and Office 365 accounts will be suspended after the final work day, unless HR or the ISO approves additional access.

Asset Disposal

SAU 39 will maintain a process for physical asset disposal in accordance with School Board Policy. The SAU 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 SAU 39 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 SAU administrative procedure EHB-R delineates the timeline for data retention for all SAU data. The SAU 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 SAU will test near-line and off-site backups of critical systems quarterly.

Disaster Recovery

The SAU's Technology Disaster Recovery Plan outlines critical staff, responsibilities, and processes in the event of a disaster or critical data loss. SAU 39 shall maintain a list of all critical systems and data, including contact information. The Technology Disaster Recovery Plan shall include processes that enable the SAU 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 SAU 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 SAU 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), SAU 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 SAU is prohibited by law, policy or contract from

disclosing or that the SAU 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 SAU operations and that must be accurately and securely maintained to avoid disruption to SAU 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 SAU 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 Officer (ISO) is 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 ISO 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 SAU 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 ISO 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/xxxi/359-c/359-c-19.htm) Notice of Security Breach - Definitions
- NH RSA 359-C:20 (http://www.gencourt.state.nh.us/rsa/html/xxxi/359-c/359-c-20.htm) Notice of Security Breach Required
- NH RSA 359-C:21 (http://www.gencourt.state.nh.us/rsa/html/xxxi/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 on the SAU 39 Technology website. An online request form is required for any new digital resources that either has an associated cost or collects staff or student data. 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 ISO 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 creating 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 SAU mission 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 for security/privacy by the Director of Technology, or designee, prior to adoption. 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
    - Evaluate terms of service, privacy policy, and MOU/contract that meet the following criteria:
        - The SAU continues to own the data shared, and all data must be available to the SAU upon request.
        - The vendor's access to and use of SAU 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 SAU. If metadata is collected, it will be protected to the same extent as the SAU's confidential or critical information.
        - SAU 39 data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
        - The provider will comply with SAU guidelines for data transfer or destruction when contractual agreement is terminated.
        - No API will be implemented without full consent of the SAU.
        - All data will be treated in accordance to federal, state and local regulations
        - The provider assumes liability and provides appropriate notification in the event of a data breach.

  Note: Exceptions can be made by the ISO 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 SAU 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 and can be accessed from the SAU 39 Technology website.
- It is the responsibility of staff to submit a request to the Digital Resource Workflow Process 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 SAU owned devices or used as part of SAU business or instructional practices.

Digital Resource Licensing/Use

All computer software licensed or purchased for SAU use is the property of the SAU 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 SAU resources that create, collect or use personally identifiable information (PII) are to be used.
- SAU software licenses will be:
    - accurate, up to date, and adequate
    - in compliance with all copyright laws and regulations
    - in compliance with SAU, state and federal guidelines for data security
- Software installed on SAU 39 systems and other electronic devices will have a current license 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 SAU 39 administrative level.

Appendix D - Data Security Checklist

A thorough risk analysis of all SAU 39 data networks, systems, policies, and procedures shall be conducted on a bi-annual basis or 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 SAU network. An internal audit of SAU network security will be conducted annually by SAU 39 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 SAU 39 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 SAU network access
- Access controls including password security (can SAU password requirements be enforced)
- Authentication methods (LDAP/Active Directory, Single Sign On, SAU 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 SAU data security requirements
- Provider has adequate data security measures including data management and incident response
- Ability to ensure proper access controls including password security (i.e. - can SAU password requirements be enforced)
- Authentication methods (LDAP/Active Directory, Single Sign On, SAU 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
- 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 SAU 39, 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 SAU and in some cases within affiliated stakeholders. This type of information is already widely distributed within the SAU, 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. SAU 39 designates the following items as directory information:

- Student's name
- Address
- Telephone listing
- Electronic mail address
- Photograph
- Date and place of birth
- Field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received
- The most recent educational agency or institution attended

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

Public Information

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

This information may be disclosed outside of the SAU.

Appendix F - Securing Data at Rest and Transit

All staff and students that log into a SAU owned computer system 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. Certain data stored on local devices may NOT be backed up by the SAU's backup solution. Staff and students will also have a mapped personal folder. This folder acts as a redirection of document folders to SAU file servers (OneDrive and/or G Suite Google Drive may be included or substituted). Access to these files is restricted to the folder's owner (staff or student who is assigned) and SAU enterprise administrator accounts. Staff and students may have limited local storage capabilities.

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 SAU 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 an Office 365 account and a G Suite for Education account that provides storage. Users are responsible for all digital content on their SAU provided accounts. 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 applications 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 SAU and meet SAU student data and data security standards.
- When exiting the SAU, students should responsibly copy their content to their own personal storage solution.
- When exiting the SAU, 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' SAU provided accounts with appropriate security settings. Users may not post this data to other cloud sharing platforms without consent of SAU administration.
- Staff should never post any documents containing classified, confidential, or restricted information to any cloud storage including SAU 39 provided Office 365 and/or Google Drive accounts without SAU approval.
- All users shall immediately report any cloud storage security problems of the SAU'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 SAU technology, staff, students, and other 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 SAU 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 SAU'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 SAU recognizes the advantages for staff and students to maintain information on these devices, users are strongly encouraged to rely on their SAU provided Office 365 and G Suite for Education Drive accounts for all storage needs. When using external storage devices, staff and students must adhere to the following guidelines:

- Users are responsible for all content on external storage devices that have been connected to SAU technology resources.
- Users must ensure that they will not introduce harmful software including computer viruses, malware, non-SAU approved software, or hacking tools to SAU 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 containing PII or confidential information 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 SAU approval.
- Regular transmission of student data to services including but not limited to the SAU Library Management system, Food Service Management system and Single-Sign-On Provider system is managed by the technology department using a secure data transfer protocol. All such services are approved by a SAU/building administrator and the Director of Technology.

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 SAU systems or in written form. All cardholder data may only be entered in secured payment systems approved by the SAU. Any cardholder data collected in written form must be shredded immediately after entry into approved system.
- The SAU 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.
- If payment information is collected via a physical form, that form must be shredded, or payment information redacted immediately upon receipt and entry into payment system.

Appendix G - Physical Security Controls

The following physical security controls shall be adhered to:

- Network systems shall be installed in an access-controlled area. The area in and around the 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 SAU 39 approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology group.
- 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 H: 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 SAU 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. It is the responsibility of the technology department to update the inventory system to reflect any in-school transfers, in-SAU transfers, or other location changes for SAU technology assets.

Disposal Guidelines

Assets shall be considered for disposal in accordance with state/federal regulations and School Board Policy. 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 Director of Technology shall approve disposals of any SAU 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 SAU 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 SAU.

A SAU-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 SAU 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 SAU. SAU 39 will not support or repair any equipment that is donated. In addition, software licenses are not transferred outside the SAU. Therefore, systems must be returned to factory installation prior to donation.

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

Virus, Malware, and Spyware Protection

SAU 39 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. SAU 39 views Internet filtering as a way to balance safety with learning, letting good content, resources, and connections in while blocking potentially inappropriate content. To balance educational Internet resource and application use with student safety and network security, the Internet traffic from all devices on the SAU network is routed through the SAU 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 Barracuda spam filters and advanced threat protection services.

Security Patches

Server patch management is performed regularly. Security patches are applied on an as needed basis..

Appendix J - Account Management

Access controls are essential for data security and integrity. SAU 39 maintains a strict process for the creation and termination of SAU 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 SAU 39, 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 group. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology group 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 SAU administrator responsible for the system (data manager) and the Director of Technology.
- When a staff member's employment is ended, either by termination or resignation, account permissions are revoked in one of two ways.
    - In the event of termination, HR will notify the Technology Department via email or phone call requiring the account to be disabled at once, preventing any further access to SAU 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 SAU resources.
    - In the event that a user having elevated permissions to any system separates from the SAU, additional measures are taken to ensure that all elevated accounts to those systems are secure.

Local/Domain Administrator Access

Only members of the SAU 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 SAU's network from outside is strictly prohibited without explicit authorization from the ISO. Remote access will be granted through virtual private network (VPN) connection through the SAU's network VPN system; no other method of remote access shall be granted without explicit authorization from the ISO. 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 SAU's network.

In the event that external access is needed by a contractor/vendor, access must be approved by the ISO. The Network Administrator will establish the contractor account, only granting access to the server/application that the contractor/vendor supports.

All external accounts will be reviewed at least annually.

Contractors/Vendors

Access to contractors/vendors is governed through the same process using School Board Policy EHAB. All contractor/vendor access must be approved by the ISO. All contractors doing business on SAU premises must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing SAU data will be assigned services based on function. Once the approval has been obtained, the technology department will create the account.

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

Staff are entered into the SAU 39 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

SAU 39 Email Address

Primary Alert Phone Number and Cell phone number

Access accounts for the SAU's SIS are setup based on staff role/position, building and required access to student data and are assigned by the Director of Technology or designee. 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 to. Administrative accounts are created based on the staff member's role/position and function and further restrictions to data are controlled through the SIS permissions functionality. 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

- Administrators/Principals/Deans
- Admin Read Only
- Athletic
- Counselors
- General User View Only
- Registrar
- School Nurses
- School Admin
- Special Education
- Teacher
- Unassigned - no access

Financial System

All staff members are entered into the SAU's financial system for the purpose of staff payroll and HR tracking. 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
- Accounts Payable
- Business Admin
- Directors
- Facilities Managers
- HR
- Office Managers
- Payroll

- Principals
- Prof. Dev.
- Remote Requisitions- (admin assistants, IT, Librarian)
- SAA
- Technology

Within each Connection Group, every user's security can be assigned a "Payroll User Role" and the options we are using for that are:

- None
- Full Access
- HR User
- Payroll User
- View Only Limited

Special Education System

The State of New Hampshire provides the SAU access to the NH Special Education Information System (NHSEIS) that houses all student IEP information. Account access to NHSEIS is maintained by the SAU Director of Special Services office in collaboration with the i4See Coordinator 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:

- School Administrator
- Provider
- Case Manager
- SAU IT Administrator
- IEP Team Member
- SAU Administrator
- SAU System Administrator
- SAU System Staff
- General Ed Teacher
- SAU Administrator

The following user roles access NHSEIS through the MyNHDOE portal: Case Manager, SAU Administrator, SAU IT Administrator, SAU Administrator, SAU System Administrator, SAU System Staff, and School Administrator. The remaining user roles, Provider, General Ed Teacher and IEP Team Member access NHSEIS through a SAU specific web address.

EDMS (Education Data Management System) houses documentation related to the special education process including student details, evaluation information, meeting minutes and related documents. It is accessible to in-district users as assigned by the SAU Office of Student Services roles: Administrator, Case Manager, Evaluator, Service Provider, Teacher, Team Leader
XLogs supports data management relative to special education service providers in areas billable and reimbursable by Medicaid to schools or Special Education aid.

Health Software System

School Nurses, Nurse Substitutes and Technology Staff are the only staff members granted access to the SAU 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.

Security Roles

- Nurse Administrator
- Nurse
- Health Care Asssistnt

Food Services System

The SAU 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

- Enterprise POS Manager
- Building POS Manager
- Cashier

Appendix L - Password Security

The SAU requires the use of strictly controlled passwords for network access and for access to secure sites and information. All passwords to SAU 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 SAU network access as outlined below.
- Passwords shall never be saved when prompted by any application with the exception of single sign-on (SSO) 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.

SAU network access to resources managed through LDAP/SSO:

- Passwords must be "strong," and must be a minimum of 10 characters long
- Passwords will only be changed in the event the user shares their password with another staff member or they believe their account has been compromised.
- Your password must not be too similar to your username.
- Do not use your SAU password for any non-SAU 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 ten consecutive invalid passwords are given. The user account will remain locked until a member of the Department of Technology unlocks the account.

Appendix M - Technology Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable SAU 39 to respond effectively and efficiently to a natural disaster or critical failure of the SAU'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 SAU's critical systems and data.
- Maintain essential technology resources critical to the day to day operations of the SAU.
- 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 SAU 39'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 have adequate storage to recover systems.
- SAU data is housed at SAU data center and backed up offsite.
- SAU data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, SAU networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

SAU 39 has appointed the following people to the disaster recovery/critical failure team: Director of Technology, Lead Network/System Administrator, Building Network Administrators, Desktop Support Staff, SAU 39 Data Coordinator and SHS Operations Manager.

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 SAU 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 SAU's data center. 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 Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent's Leadership Team will assume the role of IRM, with assistance from the IRT.

Notification

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

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- SAU 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/Communication services
- 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 SAU back online in the least amount of time possible:

- Maintained spreadsheet listing all server names, physical and virtual, and their function. A hard copy of this document will be secured at the office of the Director of Technology. An electronic version will be housed in the SAU 39 SharePoint site.
- 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 SAU data center backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and in an offsite building (future implementation will include cloud backup). The SAU's critical virtual servers can be run directly from the cloud with limited access.

Deactivation

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

Evaluation

An internal evaluation of the SAU 39 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 SAU 39 to respond effectively and efficiently to an actual or suspected data breach involving personally identifiable information (PII), confidential or protected information, SAU 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 the SAU 39 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.
- SAU data is backed up.
- Some SAU data is hosted by 3rd party providers.

Data Breach/Incident Response Team

SAU 39 has appointed the following people to the data breach/incident response team: Director of Technology, Lead Network/System Administrator, Building Network Administrators, and Technology Supports Specialists.

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 SAU.
- 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, Assistant Superintendent and Business Administrator.
- Coordinate with Superintendent to ensure communication with SAU 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, SAU data breach insurance provider, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Oversight of TDBP implementation debrief.

Activation

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

- A data breach has occurred. 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 Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Superintendent's Leadership Team 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 Director of Technology 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
- SAU and 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/Communication Subscriptions
- Radio or Television
- Written Notice
- Phone

The TDBP team will work with 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 office of the Director of Technology. An electronic version will be housed on the Technology Group SharePoint site.
- Data dictionary of all SAU hosted information systems. A hard copy of this document will be secured at the office of the Director of Technology. 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. A hard copy of this document will be secured at the technology office. An electronic version will be housed on the Technology Group SharePoint site.
- 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 SAU 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 Director of Technology, Lead Network System Administrator, Building Network Administrators, and Technology Supports Specialists. Additional members of the SAU 39 administrative team and technology group 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 IRM 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 IRM. 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 SAU administration. The types of communication will include, but not limited to, email, text message, postal mail, substitute notice and/or phone call.
- The IRM, 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 SAU 39 TDBP response will be conducted. The IRT, in conjunction with the IRM 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.