



Thursday, June 2, 2022

AGENDA

Regular Business Meeting – 7:00 PM
SAU 106 Boardroom

Christopher K. Kellan, Superintendent
Steven Finnegan, Chair
Kristin Savage, Vice Chair

1. 7:00 PM Call to Order – Chair
2. Roll Call – Clerk
3. Pledge of Allegiance
4. Approval of Minutes
5. Delegates and Individuals
6. Current Business
 - a. 7:05 PM Middle School Passion Projects - INFORMATIONAL
 - b. 7:10 PM First Day of School - INFORMATIONAL
 - c. 7:15 PM Budget Transfer - ACTION
 - d. 7:20 PM TRSD Tuition Rates - ACTION
 - e. 7:25 PM Food Service Pricing - INFORMATIONAL
 - f. 7:30 PM Data Governance Plan - INFORMATIONAL
 - g. 7:35 PM Career Technical Education - INFORMATIONAL
 - h. 7:40 PM Plaistow Waterline and Paving Projects - INFORMATIONAL
 - i. 7:45 PM Hiring Employees and Contracts - INFORMATIONAL
 - j. 7:50 PM Policies - ACTION
 - k. 7:55 PM Board Goals - INFORMATIONAL
7. 8:05 PM Administrator's Report
8. 8:10 PM Personnel Report
9. 8:15 PM Committee Reports/Reports of the School Board
10. Correspondence Folder
11. Vendor and Payroll Registers
12. 8:30 PM Other Business
13. Nonpublic Session
14. Future Dates

<i>Date</i>	<i>Time</i>	<i>Meeting Type</i>	<i>Location</i>
June 16	7:00 PM	Regular Business	SAU 106 Boardroom
July 14	7:00 PM	Regular Business	SAU 106 Boardroom
August 18	7:00 PM	Regular Business	SAU 106 Boardroom
September 1	7:00 PM	Regular Business	SAU 106 Boardroom



BUSINESS MEETING AGENDA

1-3. OPEN MEETING

4. **APPROVAL OF MINUTES** (3 set of public meeting minutes 4/21/22, 5/5/22, & 5/19/22; 2 sets of nonpublic meeting minutes)

5. **DELEGATES AND INDIVIDUALS**

6. **CURRENT BUSINESS**

a. **Middle School Passion Projects**

Middle School students will present their passion projects to improve their school.

b. **First Day of School**

Announcement of the first day of school is August 29, 2022.

c. **Budget Transfer**

Motion to transfer funds to move the elementary teaching position from Danville Elementary to Sandown North.

d. **TRSD Tuition Rates**

Motion to approve the 2022-2023 TRSD Tuition rates.

e. **Food Service Pricing**

Review the increase in school breakfast and lunch pricing.

f. **Data Governance Plan**

Review the Data Governance Plan. Action will be required at the 6/16/22 School Board meeting.

g. **Career Technical Education**

Discuss TRSD's CTE program's criteria, assessment, and enrollment.

h. **Plaistow Waterline and Paving Projects**

Karl Ingolsby to present an update on the Plaistow Waterline Tie-In and paving projects.

i. **Hiring Employees and Contracts**

Review the data reported of the current employees who have declined their contracts and amount of TRSD employment vacancies.

j. **Policies**

Motion on Policies ADC and IHCA.

k. **School Board Goals**

Review the preliminary School Board Goals for suggestions and revisions.

7. **ADMINISTRATOR'S REPORT**

Christopher K. Kellan to present.

8. **PERSONNEL REPORT**

9. **COMMITTEE REPORTS/REPORTS OF THE SCHOOL BOARD** – Board members to submit requests to serve on district committees for Chair consideration at the next board meeting.

10. **CORRESPONDENCE** – All correspondence now forwarded to board members as it comes in.

11. **VENDOR AND PAYROLL REGISTERS** – please be sure to review and sign electronically vendor and payroll registers.

12. **OTHER BUSINESS** – Board members to provide agenda items for future meeting consideration.

13. **NONPUBLIC SESSION** – If needed.

14. **FUTURE DATES** – As indicated.



June 2, 2022

Budget Transfer Request

A budget transfers is being requested which exceed the \$25,000 transfer amount pursuant to policy DBJ 'Transfer of Appropriations' and will require School Board approval. A copy of said policy is attached for your convenience.

1. From account: 100.1100.112.25.10.1 (Danville Elementary)
To account: 100.1100.112.25.12.1 (Sandown North)
Amount: \$61,266
Reason: Transfer funds to move the elementary teaching position from Danville Elementary to Sandown North

If this transfer meet with your approval, kindly accept the same by Motion and Vote. Should it be easier, feel free to motion to accept "the budget transfer in the amount and account specified in the CFO/BA's budget transfer request dated June 2, 2022".

I am happy to address any questions you may have.

Respectfully Submitted By:
Maria Watkins, CFO/Business Administrator

Timberlane Regional School District	Policy Code: DBJ
Adopted: 10-07-99 Revised: 04-16-09 Revised: 11-06-14	Page 1 of 1

TRANSFER OF APPROPRIATION (FUNDS)

Although it is the intent of the School Board to limit its spending to the amount specified for each account, in the event it becomes necessary to expend an amount greater than what was appropriated for a specific purpose, the Board is authorized to transfer funds from an unexpended balance of one appropriation to a different appropriation. All transfers of appropriations will be made consistent with the provisions of RSA 32.

The Board authorizes the Superintendent or Business Administrator to transfer funds between function object codes (7-digit code) up to \$25,000. Any transfer in excess of \$25,000 shall first require Board approval and authorization. Any transfer of funds between line items by the Superintendent shall be done so only to achieve purposes set forth the goals or aims to be accomplished through the expenditure of public funds.

Excess funds may not be transferred from the Unemployment Compensation line item.

The Superintendent is authorized to develop administrative rules or regulations to accompany this Policy.

Statutory Reference:

RSA 32
 RSA 282-A:71, III



Memo

To: Christopher K. Kellan
From: Maria Watkins
Date: June 2, 2022
Re: Timberlane Regional School District Tuition Rates

Listed below are the 2022-2023 tuition rates. Please have the School Board review and approve these rates at their next meeting.

I have calculated the following rates:

Kindergarten	10,500
Elementary	20,600
Middle School	19,300
High School	19,800
Special Education*	40,100

Previous Tuition Rates

	<u>2021-22</u>	<u>2020-21</u>	<u>2019-20</u>
Kindergarten	9,300	8,900	8,600
Elementary	18,600	17,800	17,300
Middle School	17,900	17,800	17,700
High School	19,000	18,000	17,600
Special Education*	37,100	35,800	35,000

**Special Education rate does not include costs associated with specialized services, specialized transportation, or one-to-one assistance*

Respectfully Submitted By:

Maria Watkins,
CFO/Business Administrator

Timberlane Regional School District	Policy Code: JFAB
Adopted: 05-21-87 Reaffirmed: 06-06-91 Revised: 05 02-96, 02-24-05 11-03-05, 02-16-07, 06-04-09, 10-21-10, 06-05-14, 07-25-19	Page 1 of 4

ADMISSION OF TUITION AND NON-RESIDENT STUDENTS

Related policies: JFABB, JFABD

I. Residency

Residency for the purpose of enrollment in the Timberlane Regional School District (hereafter referred to as the District) shall be defined by RSA 193:12. Any student who meets the RSA 193:12 definition of legal resident of this District is entitled to attend school in this District. A student who is not a legal resident of the District may attend school in the District only with the consent of the Superintendent. Disputes regarding residency shall be determined by the relevant laws in effect at the time.

II. Admission of Non-Resident Students

Individual non-resident students may be considered for admission to the District and only under the following conditions:

1. A resident student who moves from the District during the school year may continue as a non-resident student through the end of the school year. The District of Residence must agree to pay the tuition rate (as calculated in Section III), prorated for the time that they are not legal residents of the District. However, if the resident student moves from the District after March 31, the tuition will be waived.
2. Students from other countries, who are the guests of District residents and participating in a federally recognized education exchange program, may be admitted if space is available. Admitted students will not be charged tuition.
3. Students from other countries not participating in federally recognized education exchange program may be admitted if space is available. Admitted students shall be charged full tuition. The Timberlane Regional School District will follow Homeland Security guidelines of the federal government standards with regard to all foreign exchange students. Students must meet all of the required standards of the State of New Hampshire and the federal government in order to be accepted into the school district. ESOL instruction shall be the responsibility of the parent or guardian.
4. Children of non-resident parents, who will be moving into the District during the school year, may be admitted prior to actual establishment of residency, provided a written request and verification of the anticipated date of residency are submitted to and approved by the Superintendent. There must also be an agreement between the District and the student's school district of residence and/or parents or legal guardian regarding payment of tuition (as calculated in Section III), prorated, and special education costs for the period of time that the student is not a resident of the District. Such request shall be supported by appropriate documentation such as a

<p>Timberlane Regional School District</p>	<p>Policy Code: JFAB</p>
<p>Adopted: 05-21-87 Reaffirmed: 06-06-91 Revised: 05 02-96, 02-24-05 11-03-05, 02-16-07, 06-04-09, 10-21-10, 06-05-14, 07-25-19</p>	<p>Page 2 of 4</p>

bona fide lease or purchase and sales agreement, properly executed. If the lease or purchase and sales agreement indicate that residency will be established within 60 school days of the date the student is enrolled, the need for an agreement with District of Residence will be waived. Tuition will also be waived for the 60 days.

5. A student who has been identified homeless by the District McKinney-Vento (Homeless) Liaison shall be allowed to attend a District school pursuant to Policy JFABD (Admission of McKinney-Vento (homeless) Students).
6. Children of non-resident faculty and staff members, who are employed for at least 181 days annually, may be accepted on a space-available basis with a reduction in tuition of \$10,000. Applications may be made in writing to the Superintendent of Schools; the date of receipt of the application will determine eligibility in instances where space is restricted.
7. If a student's parents are divorced and the student lives primarily out-of-district, the student may nonetheless attend schools within the District and be considered a resident of the District for school attendance purposes provided: (1) the divorce decree allows the student to attend the District; (2) or provided the parents have agreed in writing that the student may attend the District and such written agreement is provided to the District. Students in this situation will not be charged tuition.

In a divorce decree, or parenting plan developed pursuant to RSA 461-A, a child's legal residence for school attendance purposes may be the school district in which either parent resides, provided the parents agree in writing to the district the child will attend and each parent furnishes a copy of the agreement to the school district in which the parent resides. Transportation will not necessarily be provided for students admitted under this provision and under corresponding law. The Superintendent or designee will make all determinations as to whether transportation will be provided in such circumstances.

Admission may be denied to any non-resident student who has been suspended or expelled, or involved in suspension or expulsion proceedings, in another district or whose behavior while a student in the District has had, in the sole judgment of the Superintendent, a negative impact on the resident students of the District. The decision to admit each non-resident student shall be made annually by the Superintendent.

Upon the admission of a non-resident student to the District, the Superintendent or designee will immediately notify the student's school district of residence of the student's name, date of birth, address, and grade assignment of the student. This notification shall also be made at the beginning of each school year for which the student is enrolled.

<p>Timberlane Regional School District</p>	<p>Policy Code: JFAB</p>
<p>Adopted: 05-21-87 Reaffirmed: 06-06-91 Revised: 05 02-96, 02-24-05 11-03-05, 02-16-07, 06-04-09, 10-21-10, 06-05-14, 07-25-19</p>	<p>Page 3 of 4</p>

III. Tuition of Non-Resident Students

The tuition rate will be approved by the School Board. A signed tuition confirmation letter, approved by the Superintendent, shall be on file in the SAU 106 office prior to attendance. Tuition, where applicable, shall be prepaid in monthly or quarterly payments by the district of residence or parent responsible for payments, or if appropriate, through payroll deduction. Tuition shall not be reimbursed if the student leaves the District, voluntarily or involuntarily, during the period for which payment has already been made. Failure to pay tuition as due shall be grounds for revoking the admission of non-resident tuition students. When a district of residence is responsible for tuition, approval must be that district's school board. Section IV below outlines limited special circumstances under which tuition may be waived.

IV. Responsibility for Services not Included in the Calculation of Tuition Rate

The District will not provide transportation to any non-resident student. The Board acknowledges the provisions of RSA 193:3 which state that the district in which the student resides shall retain all responsibility for the provision of special education and related services pursuant to RSA 186-C. The District's decision on whether to enroll a non-resident student will not be based, in whole or in part, on whether that student is a student with a disability, as defined by applicable state or federal law. Section V and VI below outline limited special circumstances under which this Section IV requirement for an agreement with the district of residence may be waived.

V. Tuition Agreements with other School Districts

The District may enter into one or more agreements with other school districts or agencies for the admission of non-resident students with payment of tuition by the sending district or agency. The admission of such students under these circumstances shall be governed by the terms of said agreements.

VI. Other Situations

Families who are enrolled as non-resident students at the time of the adoption of this policy will be "grandfathered" and allowed to continue attendance until they have completed their education in this District. However, the Superintendent may discontinue a student's attendance based upon the existence of disciplinary issues.

The provisions of this policy may be modified on a case-by-case basis, as needed, pursuant to separate contracts, agreements and other binding arrangements. It is not possible to anticipate all situations that may arise, thus, notwithstanding any provisions of this policy, the Timberlane Regional School District reserves the right to charge tuition or to deny admission to any non-resident student. The Timberlane Regional School District also reserves the right to admit non-resident students who don't meet the seven conditions. The Board also reserves the right to waive tuition in situations not discussed in this policy.

JFAB - ADMISSION OF TUITION STUDENTS

Timberlane Regional School District	Policy Code: JFAB
Adopted: 05-21-87 Reaffirmed: 06-06-91 Revised: 05 02-96, 02-24-05 11-03-05, 02-16-07, 06-04-09, 10-21-10, 06-05-14, 07-25-19	Page 4 of 4

Statutory References:

193:3 Change of School or Assignment

RSA 193:12 Legal Residence Required

RSA 186-C:13 Special Education: Liability for Expenses



EXECUTIVE SUMMARY

June 2, 2022

School Food Service Pricing Increase Request

Periodically, School Districts review their school breakfast and lunch pricing. Timberlane has been able to keep its meal pricing reasonable for the families of students in our District. Since the start of the 2015-2016 school year, our lunch prices have increased by only \$0.10 for paid lunches.

In order to generate the revenue necessary to continue to keep our food service program viable, District Administration is requesting paid lunch prices be increased by \$0.40 starting in the 2022-2023 School Year.

A listing of proposed lunch prices is below, along with some history of previous pricing.

	Proposed 2022-2023	2019-2020	2015-2019
Elementary School	\$3.00	\$2.60	\$2.50
Middle School	\$3.50	\$3.10	\$3.00
High School	\$3.75	\$3.35	\$3.25

Respectfully Submitted By:

Maria Watkins, CFO/Business Administrator

Timberlane Regional School District



Data Governance Manual

Timberlane Regional School District 2022

Adopted by
Timberlane Regional School Board
TBD

Contents

Introduction

Data Governance Team

Purpose

Scope

Regulatory Compliance

Data User Compliance

Data Lifecycle

Identifying Need & Assessing Systems for District Requirements

New Systems

Review of Existing Systems

Acquisition and Creation

Management and Storage

Systems Security

Data Management

Data Classification and Inventory

Security/Protection

Risk

Management

Security Logs

Physical Security Controls

Inventory Management

Virus, Malware, Spyware, Phishing and SPAM Protection

Electronic Access Security Controls

Securing Data at Rest and Transit

Usage and Dissemination

Data Storage and Transmission

Training

Archival and Destruction

District Data Destruction Processes

Asset Disposal

Critical Incident Response

Business Continuity

Disaster Recovery

Data Breach Response

Appendix A - Definitions

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

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

[Appendix D - Data Security Checklist](#)

[Appendix E - Data Classification Levels](#)

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

[Appendix G - Physical Security Controls](#)

[Appendix H - Asset Management](#)

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

[Appendix J - Account Management](#)

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

[Appendix L - Password Security](#)

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

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

Introduction

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

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

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

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

Data Governance Team

The Timberlane Regional School District's Data Governance team consists of the following positions: Superintendent, Assistant Superintendent, Business Administrator, Facilities Director, Human Resources Manager, Director of ~~Student Services and~~ Special Education, Student Services Coordinator, Director of Curriculum and Professional Learning, ~~Director of Assessment and Accountability~~, 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 Business Administrator is the district's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available. All members of the district administrative team will serve in an advisory capacity as needed.

Purpose

The School Board recognizes the value and importance of a wide range of technologies for a well-rounded education, enhancing the educational opportunities and achievement of students. The Timberlane Regional School District 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 promote the educational objectives of Timberlane Regional School District.

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

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

into place by the district.

Scope

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

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

Regulatory Compliance

The district will abide by any law, statutory, regulatory, or contractual obligations affecting its data systems (see Appendix B: Laws, Statutory, and Regulatory Security Requirements). The Timberlane Regional School District complies with the [NH Minimum Standards for Privacy and Security of Student and Employee Data](#) established in April, 2019. The Timberlane Regional School District complies with all other applicable regulatory acts including but not limited to the following:

- Children’s Internet Protection Act ([CIPA](#))
- Children’s Online Privacy Protection Act ([COPPA](#))
- Family Educational Rights and Privacy Act ([FERPA](#))
- Health Insurance Portability and Accountability Act ([HIPAA](#))
- Payment Card Industry Data Security Standard ([PCI DSS](#))
- Protection of Pupil Rights Amendment ([PPRA](#))
- Individuals with Disabilities in Education Act ([IDEA](#))
- New Hampshire State RSA - Student and Teacher Information Protection and Privacy

[NH RSA 189:65](#) Definitions

[NH RSA 189:66](#) Data Inventory and Policies

Publication [NH RSA 189:67](#) Limits on Disclosure of

Information [NH 189:68](#) Student Privacy

[NH RSA 189:68-a](#) - Student Online Personal Information

- [New Hampshire Minimum Standards for Privacy and Security of Student and Employee Data](#)
- New Hampshire State RSA - Right to Privacy:
 - [NH RSA 359-C:19](#) - Notice of Security Breach - Definitions
 - [NH RSA 359-C:20](#) - Notice of Security Breach Required
 - [NH RSA 359-C:21](#) - Notice of Security Breach Violation

Data User Compliance

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

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

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

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

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

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

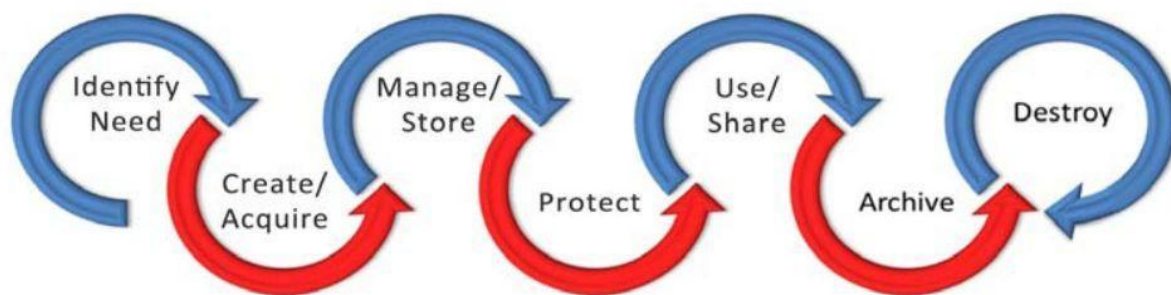
Possible disciplinary/corrective action may be instituted for, but is not limited to, the following:

- Unauthorized disclosure of PII or Confidential Information.
- Sharing your user IDs or passwords with others (exception for authorized technology staff for the purpose of support)

- Applying for a user ID under false pretenses or using another person's ID or password.
- Unauthorized use of an authorized password to invade student or staff privacy by examining records or information for which there has been no request for review. **Staff may assist in troubleshooting student access to district resources when required.**
- The unauthorized copying of system files.
- Attempting to secure a higher level of privilege without authorization.
- Installation or use of unlicensed software or software not approved for district technological systems.
- The intentional unauthorized altering, destruction, or disposal of district information, data and/or systems. This includes the unauthorized removal of technological systems such as but not limited to: laptops, internal or external storage, computers, servers, backups or other media, that may contain PII or confidential information.
- The introduction of computer viruses, hacking tools or other disruptive or destructive programs.

Data Lifecycle

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



Identifying Need & Assessing Systems for District Requirements

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

New Systems

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

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 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:
 - o The district continues to own the data shared, and all data must be available to the district upon request.
 - o The vendor's access to and use of district data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.
 - o District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
 - o The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
 - o No API will be implemented without full consent of the district.
 - o All data will be treated in accordance to federal, state and local regulations
 - o The provider assumes liability and provides appropriate notification in the event of a data breach.

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

Review of Existing Systems

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

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

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

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

Acquisition and Creation

It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets district business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use. Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the Assistant Superintendent, Curriculum Directors/Deans and the ISO, or designee, prior to purchase.

The Timberlane Regional School District, starting in July 2019, will be a member of the New Hampshire Student Data Privacy Alliance (NHSDPA). The NHSDPA is a collaboration of New Hampshire school districts and law counselors that share common concerns around student privacy. This Consortium will help vet new digital resources using collective resources. The goals of this Consortium are:

- Establish a community of stakeholders who have various needs addressed through policy, technology and/or effective practice sharing around effective privacy management,
- Identify projects that have on-the-ground and real-world impact on student data privacy enabling schools, districts, state and vendors find resources, adapt them to their unique context and implement needed protections,
- Development of tools and resources to address operational issues not currently being addressed,
- Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work,
- Development of a clearinghouse of student data privacy operational issues and resources to support schools, districts, states and vendors in managing those issues – no matter where the resources originate.

Once the Consortium is operating, staff will check a database of approved digital resources to see if it has been approved for meeting or exceeding minimum standards outlined by the state. In the event it does not there will be an approval process where the staff member will submit information about the resource they would like to use on the NH Consortium website. A first level approval would need to be granted by the district in order to make sure that there are no obvious or known issues with the resource and that it passes curriculum related goals. Passing that, the Consortium will contact the vendor in order to process agreements that they will follow all minimum federal and state laws regarding security and privacy. If the provider completes all agreements the resource will be added to the database of vetted resources that are good to use.

Management and Storage

Systems Security

The district will provide access to confidential information to appropriately trained district staff and volunteers only when the district determines that such access is necessary for the performance of their duties. The district will disclose confidential information only to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law and authorized by the district (School Board Policy EHAB).

Therefore, systems access will only be given on an as-needed basis as determined by the data manager and ISO. Further information regarding Electronic Access Security Controls is contained in the

Security/Protection section of this manual.

Data Management

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

Data Managers are responsible for the development and execution of practices and procedures that ensure the accuracy and security of data in an effective manner. All district administrators are data managers for all data collected, 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 district 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 district data security guidelines.
- ensure that staff are trained in the district's proper procedure and practices in order to ensure accuracy and security of data.
- assist the ISO in enforcing district policies and procedures regarding data management.

Data Classification and Inventory

Classification is used to promote proper controls for safeguarding the confidentiality of data. Regardless of classification, the integrity and accuracy of all classifications of data are protected. The classification assigned and the related controls applied are dependent on the sensitivity of the data. Data is classified according to the most sensitive detail they include. Data recorded in several formats (e.g., 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 district data, such as student information systems, financial systems, payroll systems, transportation systems, food-service systems, email systems, instructional software applications and others. The ISO or designee will identify the data files and data elements maintained in those systems and identify confidential and critical information the district possesses or collects. Once the data files and data elements are identified, the ISO or designee will classify the data as confidential or critical so that those files and the information they contain can be more closely monitored.

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

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

- Who has access
- Criticality/Sensitivity Rating

Security/Protection

Risk Management

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

Security Logs

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

Physical Security Controls

Technology telecommunication closets are housed in secure locations. Access authorization is assigned through the 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 district shall maintain a process for inventory control in accordance to federal and state requirements and School Board policy. All district technology assets will be maintained in inventory and verified through the regular inventory verification process (see Appendix H: Asset Management).

Virus, Malware, Spyware, Phishing and SPAM Protection

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

Electronic Access Security Controls

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

policies via the Faculty Handbook sign-off form annually.

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

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

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

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

Staff Users

All new staff accounts are authorized through an HR hiring process (see Appendix J: Account Management). Role-based permissions and security groups are used to establish access to all systems (see Appendix K: Data Access Roles and Permissions). If a staff member requires additional access, a request must be made directly to the 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 district premise must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing district data will be considered on premise users. Once the approval has been obtained, the technology department will create the account, only granting access to the server/application that the contractor/vendor supports.

Password Security

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

Concurrent Sessions

When possible, the district will limit the number of concurrent sessions for a user account in a system. **The reason for doing this is to ensure that any sessions left open on another computer are terminated when a user logs in from another location.**

Remote Access

Access into the District'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 district's network VPN appliance; 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 District's network. All VPN accounts will employ the use of 2 factor authentication.

In the event that VPN access is needed by a contractor/vendor, access must be approved by the ISO. The ISO or designee will establish the contractor account, only granting access to the server/application that the contractor/vendor supports. All VPN accounts will be reviewed at least annually.

Securing Data at Rest and Transit

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

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

Usage and Dissemination

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

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

District staff, contractors and agents will notify the 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 district owned device will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on the local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. Staff and students may also have a mapped personal folder **and/or Google Drive**. This folder acts as a redirection of document and desktop folders to district file servers. Access to these files is restricted to the folder's owner (staff or student who is assigned) and district enterprise administrator accounts. Staff and students using Chromebook devices have limited local storage capabilities. Chromebook users are to store data online within their GSuite for Education Drive account.

Cloud Storage and File Sharing

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

File Transmission Practices

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

Credit Card and Electronic Payment

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

Mass Data Transfers

Downloading, uploading or transferring PII, confidential information, and internal information between systems shall be strictly controlled. Requests for mass download of, or individual requests for, information for research or any other purposes that include PII shall be reviewed and approved by the Superintendent or designee. All other mass downloads of information shall be approved by the 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. **For enhanced security, staff can print to the district's cloud print queue which only releases print jobs at district copiers by swiping their security fob.**

Oral Communications

Staff shall be aware of their surroundings when discussing PII and confidential information. This includes, but is not limited to, the use of cellular telephones in public areas. Staff shall not discuss PII or Confidential Information in public areas if the information can be overheard. Caution shall be used when conducting conversations in: semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or public areas.

Training

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

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

Archival and Destruction

Once data is no longer needed, the 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 unretrievable.

District Data Destruction Processes

The district will ~~regularly review~~ **annually** all existing data stored on district provided storage for the purposes of ensuring data identification and appropriate destruction. Data destruction processes will align with School Board Policy EHB and EHB-R. District data managers will ~~regularly review~~ **annually** 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 GSuite for Education account will be maintained 90 days after the student's final date of attendance.
- Staff GSuite for Education accounts will be suspended after the final work day, unless HR or the ISO approves a district administrator to maintain access.

Asset Disposal

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

Critical Incident Response

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

Business Continuity

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

Disaster Recovery

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

disaster, or critical system failure (see Appendix M: Disaster Recovery Plan).

Data Breach Response

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

Appendix A - Definitions

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

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

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

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

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

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

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

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

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

- following existing approval processes for the selection, budgeting, purchase, and implementation of any digital resource.

Information Security Officer: The Information Security 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 district or provider.

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

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

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

User: The user is any person who has been authorized to read, enter, print, modify, or delete 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](#) 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 Minimum Standards - FAQ’s](#)

New Hampshire State RSA Chapter 359-C 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

Draft

Appendix C - Digital Resource Acquisition and Use

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

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

New Resource Acquisition

Staff will be required to complete steps outlined under the staff section of the District's website. An online request 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 district business objectives, is in line with curriculum or behavioral standards, is age appropriate, is instructionally sound, and is appropriate for the intended use.
- Digital resources that accompany adopted instructional and/or curriculum materials will be vetted by the appropriate Assistant Superintendent, Curriculum Directors/Deans and the Director of Technology, or designee, prior to purchase.

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:
 - o The district continues to own the data shared, and all data must be available to the district upon request.
 - o The vendor's access to and use of district data is limited; the data cannot be used for marketing, targeted advertising or data mining; and the data cannot be shared with third parties unless allowed by law and authorized by the district. If metadata is collected, it will be protected to the same extent as the district's confidential or critical information.
 - o District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
 - o The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
 - o No API will be implemented without full consent of the district.
 - o All data will be treated in accordance to federal, state and local regulations
 - o The provider assumes liability and provides appropriate notification in the event of a data

breach.

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

Approved Digital Resources

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

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

Digital Resource Licensing/Use

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

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

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

Appendix D - Data Security Checklist

A thorough risk analysis of all Timberlane Regional School District data networks, systems, policies, and procedures shall be conducted on an 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 District network. An internal audit of District network security will be conducted annually by District Technology staff.

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

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

Data Security Checklist for District Hosted Systems

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

Data Security Checklist for Provider Hosted Systems

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

Appendix E - Data Classification Levels

Personally Identifiable Information (PII)

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

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

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

Confidential Information

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

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

Internal Information

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

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

Directory Information

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

- Student's name
- Address
- Telephone listing
- Electronic mail address
- Photograph
- Date and place of birth
- Major 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
- Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user
- A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.

This information may only be disclosed as permitted in School Board Policy JRA and JRA-R

Public Information

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

Appendix F - Securing Data at Rest and Transit

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

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

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the internet. All staff and students are provided with a GSuite Or Office 365 for Education account that provides adequate storage. Users are responsible for all digital content on their district provided GSuite or Office 365 for Education Drive. When using cloud storage, staff must adhere to the following guidelines:

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

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

- Users must abide by all policies and procedures regarding professional conduct and

communication when sharing, reviewing, updating, commenting and re-sharing.

- When sharing content, users must ensure that other users accessing the information in the files have appropriate access to the information based on job function.
- All users shall immediately report any inappropriate sharing of the district's technology resources to an administrator.

External Storage Devices

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

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

File Transmission Practices

- Staff are responsible for securing sensitive data for transmission through email or other channels. When possible, staff should de-identify or redact any PII or confidential information prior to transmission.
- Staff should never include a password in any electronic communication unless directed to do so by Technology Staff.
- Staff should not transmit files labeled classified, confidential, or restricted through email or third party file transfer services without district approval.
- Regular transmission of student data to services such the District Library Management system, Food Service Management system 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 district/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 district systems or in written form. All cardholder data may only be entered in secured payment systems approved by the district. Any cardholder data collected in written form must be shredded immediately after entry into the approved system.
- The district will never maintain a data system for payment information. All payment information will be stored and processed by a 3rd party accessible through a secure portal.

- Never request cardholder information to be transmitted via email or any other electronic communication system. The district will employ measures to help flag emails that contain this information.
- 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 the payment system.

Draft

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 district approved technology inventory program. No technology equipment regardless of how purchased or funded shall be moved without the explicit approval of the technology department.
- Ensure that technological equipment or systems being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures (see Appendix I: Asset Management).

Appendix H - Asset Management

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

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

Inventory

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

Disposal Guidelines

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

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

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

Methods of Disposal

Once equipment has been designated and approved for disposal, it shall be handled according to policy [DL \(School Properties Disposal Procedure\)](#).

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

Virus, Malware, and Spyware Protection

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

Internet Filtering

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

Phishing and SPAM Protection

Email is filtered for viruses, phishing, spam, and spoofing using Google and Office 365 services.

Security Patches

Server patch management is performed regularly. Security patches are applied on an as needed basis. The district utilizes a Microsoft WSUS server (Windows Server Updates Services) to distribute approved updates.

Appendix J - Account Management

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

Staff Accounts

When a staff member is hired by the Timberlane Regional School District, 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 members is sent from Human Resources to the Technology Department. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology Department creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s) (see Appendix K: Data Access Roles and Permissions).
- Any exception to permissions must be approved by the district administrator responsible for the system (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 district resources.
- In the event of resignation, HR will notify the Technology Department via email indicating the termination date. The account is disabled at the end of business on the termination date, preventing further access to district resources.
- In the event that a user having elevated permissions to any system separates from the district, additional measures are taken to ensure that all elevated accounts to those systems are secure.

Local/Domain Administrator Access

Only members of the District Technology staff will be granted access to domain level administrator and local machine administrator accounts in order to complete their job functions. **Middle school and High School administrators and counselors have the abilities to reset student accounts only at their respective schools.**

Remote Access

Access into the District'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 district's network VPN appliance; 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 District's network.

In the event that VPN 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 VPN accounts will employ the use of 2 factor authentication.

All VPN 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 HR and ISO. All contractors doing business on district premises must also pass a background check unless other security measures are addressed in a vendor contract. All contractors/vendors accessing district data will be considered on premise users. Once the approval has been obtained, the technology department will create the account.

Draft

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

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

- Building/Site location
- Status - Active
- Staff Type
- District Email Address
- Primary Alert Phone Number and Cell phone number

Access accounts for the District's SIS are setup based on staff role/position, building and required access to student data and are assigned by the 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 security groups. Security groups control access permissions to certain data sets such as attendance, demographic data, grades, discipline etc. and whether the staff member can view or maintain data. Additional page level permissions are assigned to the security groups. PowerSchool administrative accounts log into the SIS Admin Portal.

Security Groups

- Administrator
- Guidance Staff
- School Administrator
- Administrative Assistant
- School Nurses
- Unassigned - no access

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

Financial System

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

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

Financial System Security Roles

- AP/GL (Accounts Payable), General Ledger)
- AP/GL/PR (Accounts Payable, General Ledger, Payroll)
- Full Access
- HR Admin Asst
- HR Director
- HR Review

- IT Processing
- Payroll
- PR/HR (Payroll, Human Resources)
- Principals/Directors
- Remote (Admin Assistants at schools)
- Remote SPED Only

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

Special Education System

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

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

The following user roles access NHSEIS through the MyNHDOE portal: Case Manager, District Administrator, District IT Administrator, SAU District 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.

Health Software System

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

Food Services System

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

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

Appendix L - Password Security

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

- Passwords shall never be shared with another person.
- When possible, user created passwords should adhere to the same criteria as required for district network access as outlined below.
- Passwords shall never be saved when prompted by any application 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.
- Staff Passwords will be expired and forced to be changed to a strong one at least once per calendar year
- **All district administrators, SAU based employees, and school front office staff shall be required to use 2 Factor authentication for TRSD email and Google logins.**
- Student Passwords will be expired upon entering 6th and 9th grades and students will be required to choose a new strong one.

District network access to resources managed through Active Directory/Google Accounts:

- Passwords must be “strong,” and must be a minimum of 8 characters long, must include at least one uppercase character, one number and one special character (! @ # \$ % & ?)
- Passwords will only be changed in the event the user shares their password with another staff member or they believe their account has been hacked.
- Your password must not be too similar to your username.
- Do not use your district password for any non-district systems.
- Password history will be enforced so that users cannot change a password to a recently use one. Where possible, system software should enforce the following password standards:
- Passwords routed over a network shall be encrypted.
- Passwords shall be entered in a non-display field.
- System software shall enforce the changing of passwords and the minimum length.
- System software shall disable the user password when more than five consecutive invalid passwords are given.

Appendix M - Technology Disaster - Recovery Plan

OBJECTIVES

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

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

Planning Assumptions

The following planning assumptions were used in the development of Timberlane Regional'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.
- Data housed at the district data center is backed up in the cloud.
- District data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

The Timberlane Regional School District has appointed the following people to the disaster recovery/critical failure team:: Director Technology, Business Administrator, Business Operations Coordinator and all Senior Technology Specialists.

In the event the TDRP is activated, overall management of the response is delegated to this team.

Their primary responsibilities include:

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

Activation

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

- A natural disaster has occurred and affects the operation of the District's data center(s). A natural disaster includes but is not limited to the following: tornado, earthquake, lightning, and flood.
- 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, if affected, will be notified in the event the plan has been activated:

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

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

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

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

Implementation

The TDRP team has the following in place to bring the District back online in the least of 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 technology office. An electronic version will be housed on Google Drive.
- Maintained secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.
- The District's locally data backup solution includes the use of a daily local backup and off-site file storage. The local backup copy will be sent offsite for storage on a daily basis.
- The District's cloud based applications will be backed up daily and stored securely off site.

- In the event of a critical system failure, the District can restore that server back to our current environment from the backup solution.

Deactivation

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

Evaluation

An internal evaluation of the Timberlane Regional 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 the Timberlane Regional School District to respond effectively and efficiently to an actual or suspected data breach involving personally identifiable information (PII), confidential or protected information, district identifiable information and other significant cybersecurity incident. The objectives of the TDBP are:

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

Planning Assumptions

The following planning assumptions were used in the development of Timberlane Regional TDBP:

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

Data Breach/Incident Response Team

Timberlane Regional has appointed the following people to the data breach/incident response team: Director of Technology, Business Administrator, Business Operations Coordinator, Director of Human Resources, Director of Student Services and all Senior Technology 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 district itself.
- Communicate impact, the number of affected individuals, the likelihood information will be or has been used by unauthorized individuals and updates of progress to the Superintendent and Business Administrator.
- Coordinate with Superintendent to ensure communication with district staff and or parents as deemed appropriate.

- Oversight of the TDBP implementation and data breach resolution.
- Allocate and manage technology staff resources during the event.
- Work with vendors, 3rd party providers, manufacturers, legal counsel, district data breach insurance provider, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Oversight of TDBP implementation debrief.

Activation

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

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

The Information Security 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, if affected, be notified in the event the plan has been activated:

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

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

- Email
- Social Media/Website

- Radio or Television
- Written Notice
- Phone

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

Implementation

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

- Data inventory of all systems containing sensitive data. A hard copy of this document will be secured at the technology office. An electronic version will be housed on the Technology Departments Team Drive
- Data dictionary of all district hosted information systems. A hard copy of this document will be secured at the technology office. Due to non- disclosure agreements, this data may not be available in other locations/formats. The appropriate vendor(s) can be contacted for this information.
- Maintained spreadsheet listing all server names, physical and virtual, and their function. A hard copy of this document will be secured at the technology office. An electronic version will be housed on the Technology Departments Team Drive.
- Maintained secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.
- The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and 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, Business Administrator, Business Operations Coordinator, Director of Human Resources, Director of Student Services and all Senior Technology Specialist. Additional members of the Timberlane Regional School District's administrative team and technology department may be designated to assist on the IRT.
- The IRT will determine the status of the breach, on-going, active, or post-breach. For an active and ongoing breach, the IRT will initiate appropriate measures to prevent further data loss. These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.
- The IRT will work with the data managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.

- The 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 district communications team. 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 Timberlane Regional School District's 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.

TRSD 2022 Data Governance Manual Change Log

- 1.) Page 3 - remove titles of positions no longer employed by the district.
- 2.) Page 6 - Added note about staff being able to assist students with troubleshooting district access issues.
- 3.) Page 7 - Clarified that existing systems get reviewed annually.
- 4.) Page 11 - Provided clarification on why concurrent access to systems is limited when possible.
- 5.) Page 12 - Added Google drive as a destination for staff and student data.
- 6.) Page 13 - Added note about being able to send print jobs to the district cloud print queue and releasing jobs with security fob.
- 7.) Page 14 - Clarified that the district's data destruction process gets reviewed annually.
- 8.) Page 30 - Added note about middle and high school administrators and counselors being able to change student passwords at their schools.
- 9.) Page 34 - Added note that all district administrators, SAU based employees, and school front office staff will be required to use 2FA (2 Factor Authentication) for TRSD email and Google access.

Timberlane Regional School District	Policy Code: EHAB
Adopted: 06-20-19	Page 1 of 5

DATA GOVERNANCE AND SECURITY

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

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

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

A. Definitions

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

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

B. Data and Privacy Governance Plan - Administrative Procedures.

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

The Data Governance Plan shall include:

- (a) An inventory of all software applications, digital tools, and extensions. The inventory shall include users of the applications, the provider, purpose, publisher, privacy statement, and terms of use;
- (b) A review of all software applications, digital tools, and extensions and an assurance that they meet or exceed minimum standards set by the New Hampshire Department of Education;
- (c) Policies and procedures for access to data and protection of privacy for students and staff including acceptable use policy for applications, digital tools, and extensions used on District hardware, server(s) or through the District network(s);

Timberlane Regional School District	Policy Code: EHAB
Adopted: 06-20-19	Page 2 of 5

- (d) A response plan for any breach of information; and
- (e) A requirement for a service provider to meet or exceed standards for data protection and privacy.

2. Policies and Administrative Procedures. The Superintendent, in consultation with the ISO, is directed to review, modify and recommend (policies) create (administrative procedures), where necessary, relative to collecting, securing, and correctly disposing of District data (including, but not limited to Confidential and Critical Data/Information, and as otherwise necessary to implement this policy and the Data Governance Plan. Such policies and/or procedures 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 District's Information Security Officer (ISO) and reports directly to the Superintendent or designee. The ISO is responsible for implementing and enforcing the District's security policies and administrative procedures applicable to digital and other electronic data, and suggesting changes to these policies, the Data Governance Plan, and procedures to better protect the confidentiality and security of District data. The ISO will work with the both District and building level administrators and Data managers (paragraph E, below) to advocate for resources, including training, to best secure the District's data.

The Business Administrator is the District's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

D. Responsibility and Data Stewardship.

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

E. Data Managers.

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

F. Confidential and Critical Information.

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

Timberlane Regional School District	Policy Code: EHAB
Adopted: 06-20-19	Page 3 of 5

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

District employees, contractors and agents will notify the 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 the District in promptly and appropriately addressing a security breach.

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

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

G. Using Online Services and Applications.

District staff members are encouraged to research and utilize online services or applications to engage students and further the District's education mission. District employees, however, are prohibited from installing or using applications, programs or other software, or online system/website, 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

Timberlane Regional School District	Policy Code: EHAB
Adopted: 06-20-19	Page 4 of 5

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 District technology resources.

J. Consequences

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

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

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

Legal References:

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

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

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

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

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

RSA 189:65 * Definitions

RSA 186:66 * Student Information Protection and Privacy

RSA 189:67 * Limits on Disclosure of Information

RSA 189:68 * Student Privacy

RSA 189:68-a * Student Online Personal Information

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

NHSBA note, September 2018, this policy was created to reflect, in part, the requirements of RSA 189:66, V (NH Laws 2018 Chapter 252 (HB 1612)). HB 1612 also requires NHDOE to establish minimum standards for privacy and security. As of September 18, 2018, those standards have yet to be finalized. NHSBA expects that those standards will require further modifications to this policy as well as companion administrative procedures and other existing NHSBA sample policies. Additionally, because a sampling review of the existing technology policies for various district reveal wide variations from current NHSBA samples (see "Related policies" reference at the top of this sample policy EHAB). Districts adopting this sample, therefore, are advised to closely review their current technology policies for provisions which may be in conflict with provisions of this sample EHAB.

Timberlane Regional School District	Policy Code: EHAB
Adopted: 06-20-19	Page 5 of 5

NHSBA has designated this policy as "Priority/Required by Law". Technically, what is required is a Board approved Data Governance Plan, no later than June 30, 2019. However, because of the significance of the subject, and the required plan, we have determined that the policy meets the priority designation.



EXECUTIVE SUMMARY

June 2, 2022

TRSD is in a regional partnership with Salem, Pinkerton, Windham and Pelham which provides career and technical education (CTE) opportunities at Salem CTE and Pinkerton CTE. Both locations provide numerous courses and or programs that are available to students on a limited basis as there are limited seats allocated to each sending school. TRSD pays the tuition to both Salem and Pinkerton, and supplies the transportation to Salem, for each of the TRHS students who attend programs at those schools.

Junior and senior students attend TRHS for their academic classes for approximately half the day, and attend one of the CTE centers for the other half of the day. Therefore scheduling CTE students to ensure both their vocational and academic needs presents unique challenges. Often times, there are more students wishing to enroll in CTE classes than spaces available at those schools, and just like all scheduling at the high school, the computer generates the schedule based on best fit for students and staff given all of the constraints. All CTE classes have an application process, and often times the classes have prerequisites based on the student's TRHS academic classes. Similarly, many of the two-year CTE programs require grade and attendance prerequisites to move from level one in junior year to level two in senior year.

Although more students could benefit from career and technical education in the district and around the state, there are many obstacles to increasing these opportunities. As previously mentioned, all of the schools in the CTE region, have limited number of 'seats' and the program offerings are capped. This is due to space restrictions at the CTE centers and the staff that is available. Like almost all schools around the state, the CTE centers have a limited pool of qualified instructors willing to teach, and thus program offerings can be limited. Like, staffing, the space in the facilities could limit the sections and types of courses that a facility can offer. At one time, TRHS did have an extensive shop area with the ability to run courses in automotive, metal, and construction, but those spaces were converted into classrooms approximately 15 years ago. Likewise, TRHS has a kitchen to offer culinary classes, but it is not a commercial kitchen like what Salem has to offer a true professional culinary career program.

TRHS has always had good relationships with both Salem and Pinkerton CTE centers, and we look forward to continue this relationship to benefit TRHS students in the future. We will continue to advocate for student access to programs and look at creative ways to provide new and varied CTE opportunities.

Respectfully submitted,

Mark Pedersen
Barry Chooljian



EXECUTIVE SUMMARY

June 2, 2022

Pollard Elementary Water

Potable Water Cost:

The town of Plaistow confirmed that the preliminary fee schedule was approved by vote of the Board of Selectmen at their February 7, 2022, meeting. Since this is a new water system, the town has done its best to set the consumption rate and the cost using all the information available. The rates will be reviewed by the Board of Selectmen annually and adjusted as needed based on any changes to Plaistow-specific operating costs.

The current rate is \$7.00 per 1,000 gal. The actual consumption at Pollard in 2019 was 570,533 gal. so the estimated annual cost is \$4K

Cost to Remain on well:

The annual testing fee is \$3K but it could vary based on findings. We have not received the final quote for the PFOA filtration system; however it is estimated to be in the \$25K - \$32K range.

There are grants available to assist with costs to hook up to the public water supply or to address the filtration needs, due to the increased rate of local PFOA levels.

Fire System:

The current system needs to have engineering completed to ensure the fire system will be able to work correctly with the new water supply. The district also needs to install a backflow preventer that is designed for the new water supply into our fire system.

We have not received the final quote from Hampshire Fire Protection but the initial verbal, estimate was in the \$20K range. They are still working on it and have engaged a Fire Protection Engineer.

We have also asked EEI to provide us an estimate to perform the engineering and installation of the fire system.

Respectfully submitted by:

Karl Ingoldsby, Director of Plant Operations



EXECUTIVE SUMMARY

June 2, 2022

District Wide Paving Update

For your perusal below is the detail of the bid pricing for various paving projects that are needed to prevent further damage, expand use, or to make areas safe for our students and staff.

I have indicated areas that are considered safety concerns due to tripping hazards or for other reasons.

Location	Paving Project	Cost	Is this safety priority?	Price for Safety Related
High School	Greenough Road Parking	84,500	Yes	84,500
Middle School	Expand Basketball Playing Surface	19,470		
Middle School	Remove/Replace Walkway	19,500	Yes	19,500
Middle School	Additional Play Surface	19,470		
Sandown North	Additional Parking Along Entrance Driveway	21,880		
Sandown North	Pave Behind Gymnasium	42,515		
Sandown Central	Pave Cemetery Road Entrance	42,800	Yes	42,800
Sandown Central	Repair Sink Hole	20,100	Yes	20,100
Atkinson Academy	Reconstruct Access to West of Building, Alleviate drop at Entry to Lot, Basketball Court & Walkway to Boiler Room	39,500	Yes	39,500
Atkinson Academy	Repair Access Area to Dumpsters	5,500		
Atkinson Academy	Repair Damaged Parking Areas	5,880		
Danville	Repair Damaged Areas	200,671		
Pollard	Repair Damaged Areas	117,833		
Total		639,619		206,400



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

 Timberlane.net

 @TimberlaneRegional

 @TimberlaneRSD

 @TimberlaneRSD

We want to reiterate that these prices are from April, the cost of oil affects the cost of pavement, so prices may have been impacted.

We have also received several quotes to clean, crack seal, sealcoat, and repaint all parking lot markings at each of our schools. We are currently working on a plan to address these issues on a rotating basis as this will prolong the life of our paved areas.

If you would like to tour an area or have any questions, please feel free to reach out to me.

Respectfully submitted by:

Karl Ingoldsby, Director of Plant Operations

Below are photographs and Google Earth images to show areas of concern.

Danville Elementary:





NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

 Timberlane.net

 @TimberlaneRegional

 @TimberlaneRSD

 @TimberlaneRSD



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

 Timberlane.net

 @TimberlaneRegional

 @TimberlaneRSD

 @TimberlaneRSD



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

Timberlane.net

@TimberlaneRegional

@TimberlaneRSD

@TimberlaneRSD



Pollard School:



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

 Timberlane.net

 @TimberlaneRegional

 @TimberlaneRSD

 @TimberlaneRSD



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

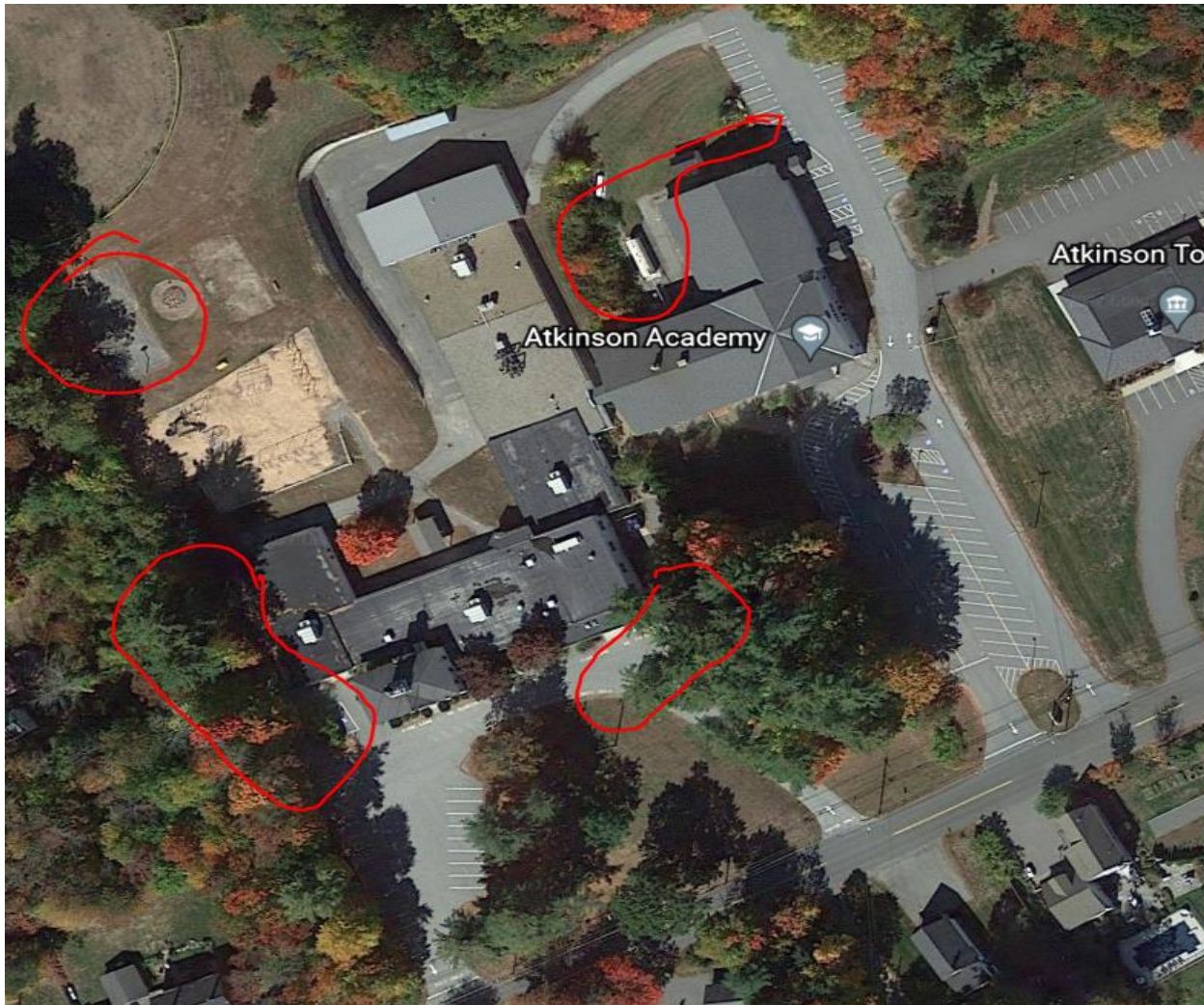
Timberlane.net

[@TimberlaneRegional](https://www.facebook.com/TimberlaneRegional)

[@TimberlaneRSD](https://www.instagram.com/TimberlaneRSD)

[@TimberlaneRSD](https://www.twitter.com/TimberlaneRSD)

Atkinson Academy:



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

 Timberlane.net

 @TimberlaneRegional

 @TimberlaneRSD

 @TimberlaneRSD





NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

Timberlane.net

@TimberlaneRegional

@TimberlaneRSD

@TimberlaneRSD





NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

Timberlane.net

@TimberlaneRegional

@TimberlaneRSD

@TimberlaneRSD

Sandown North:





NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

Timberlane.net

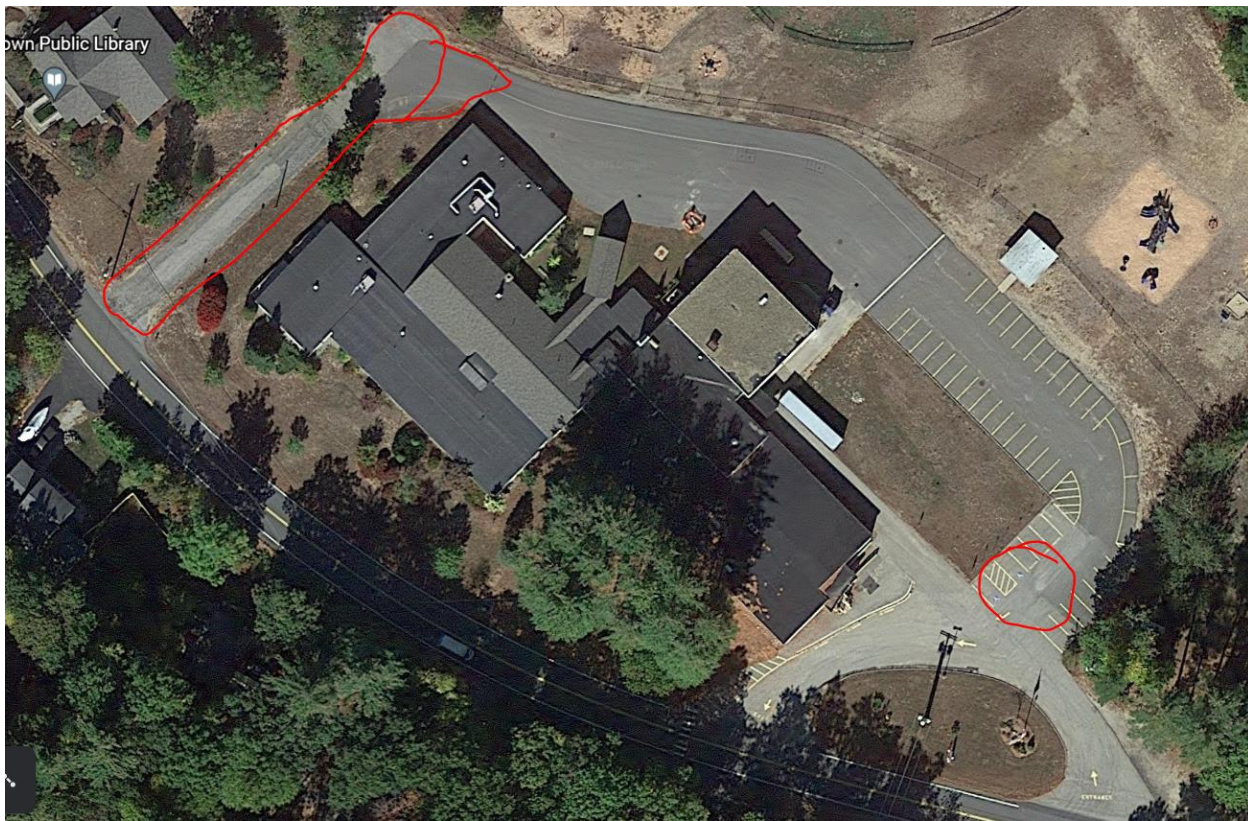
@TimberlaneRegional

@TimberlaneRSD

@TimberlaneRSD



TLC at Sandown Central:



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

Timberlane.net

@TimberlaneRegional

@TimberlaneRSD

@TimberlaneRSD



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

Timberlane.net

@TimberlaneRegional

@TimberlaneRSD

@TimberlaneRSD

Timberlane Regional Middle School:



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

[Timberlane.net](https://www.timberlane.net)

[@TimberlaneRegional](https://www.facebook.com/TimberlaneRegional)

[@TimberlaneRSD](https://www.instagram.com/TimberlaneRSD)

[@TimberlaneRSD](https://www.twitter.com/TimberlaneRSD)

Timberlane Regional High School:



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

Timberlane.net

@TimberlaneRegional

@TimberlaneRSD

@TimberlaneRSD



The mission of the Timberlane Regional School District is to engage all students in challenging and relevant opportunities, emphasizing high aspirations and personal growth.

Professionals that have gone through the Board As of May 19, 2022

Name	Position	School
1 Amy Lagasse	School Counselor	Danville
2 Kelly Graham	SPED Teacher	Danville
3 Cassondra Mello	SPED Teacher	Danville
4 Karen Reinhold	5th Grade Teacher	Pollard
5 Kristin Paulson	5th Grade Teacher	Sandown North
6 Melissa Dixey	SPED Teacher	Sandown North
7 Dr. Allyna Ward	English Language Arts Teacher	TRHS
8 Taylor Kenney	Mathematics Teacher	TRHS
9 Ashlee Sarnie	English Education	TRMS
10 Philip Balanoff	Physical Education Teacher	TRMS
11 Christopher Wiedenfeld	Physical Education Teacher	TRMS

Administrators gone through the Board As of May 19, 2022

1 Jusin Krieger	Asst Superintendent	TRSD
2 Dr. Cornelius Campbell	Asst Principal of Alt Programs	TRHS
3 Danielle Foley	Assistant Principal	TRHS
4 Erica Shovein	SPED Coordinator	TRHS
5 Maura Maher	Dir of Guidance 6-12	TRMS & TRHS



NH School Administrative Unit 106 | Timberlane Regional School District

30 Greenough Road, Plaistow, NH 03865 Voice: (603) 382-6119 Fax: (603) 382-3334

Timberlane.net

@TimberlaneRegional

@TimberlaneRSD

@TimberlaneRSD

TRSD POLICY COMMITTEE'S RECOMMENDATIONS TO THE SCHOOL BOARD

June 2, 2022

Second Read

Policy	Changes/Recommendations
ADC Tobacco Products Ban	PC recommends to adopt
IHCA Summer Learning	PC recommends to adopt

Timberlane Regional School District	Policy Code: ADC
Adopted: 07-21-83 Revised: 02-15-99 Revised: 09-11-02 Revised: 02-24-05 Reaffirmed: 11-15-12 Revised: 06-02-16 Revised:	Page 1 of 3

PROHIBITIONS REGARDING USE AND POSSESSION OF TOBACCO PRODUCTS, E-CIGARETTES AND E-LIQUIDS IN AND ON SCHOOL FACILITIES AND GROUNDS

State law prohibits the use of any tobacco product, E-cigarette, or liquid nicotine in any facility or upon any grounds maintained by the District. Students and minors are further prohibited from possessing such items in or upon any facility, school vehicle, or grounds owned or maintained by the District.

A. **Definitions.** *These definitions shall also include any amendments to the referenced statutes as the same may be amended or replaced from time to time.*

"Tobacco product(s)" means any product containing tobacco including, but not limited to, cigarettes, smoking tobacco, cigars, chewing tobacco, snuff, pipe tobacco, smokeless tobacco, and smokeless cigarettes, as well as any other product or item included in RSA 126-K:2, XI.

"Device" means any product composed of a mouthpiece, a heating element, a battery, and electronic circuits designed or used to deliver any aerosolized or vaporized substance including, but not limited to, nicotine or cannabis. Device may include, but is not limited to, hookah, e-cigarette, e-cigar, e-pipe, vape pen, e-hookah, as well as any other object or item defined in RSA 126-K:2, II-a.

"E-cigarette" means any electronic smoking device composed of a mouthpiece, a heating element, a battery, and electronic circuits that **may or may not contain** nicotine **or e-liquid**. This term shall include such devices whether they are manufactured as e-cigarettes, e-cigars, or e-pipes, or under any other product name as well as any other product or item included in RSA 126-K:2, II-b.

"E-liquid" means any liquid, oil, or wax product containing, but not limited to, nicotine or cannabis intended for use in devices used for inhalation as well as any other substance included or defined in RSA 126-K:2, II-c.

"Liquid nicotine" means any liquid product composed either in whole or in part of pure nicotine and propylene glycol and manufactured for use with e-cigarettes, as well as any other product or item included in RSA 126-K:2, III-a.

Timberlane Regional School District	Policy Code: ADC
Adopted: 07-21-83 Revised: 02-15-99 Revised: 09-11-02 Revised: 02-24-05 Reaffirmed: 11-15-12 Revised: 06-02-16 Revised:	Page 2 of 3

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

B. Students

No student shall purchase, attempt to purchase, possess or use any tobacco product, *device*, E-cigarette, *E-liquid*, or liquid nicotine in any facility, in any school vehicle or anywhere on school grounds maintained by the District.

Enforcement of the prohibition against students shall initially rest with building principals, or their designees, who may also report any violation to law enforcement, for possible juvenile, criminal or other proceedings as provided under state law. Additional consequences may be administered pursuant to printed student conduct rules.

C. Employees

No employee shall use any tobacco product, *device*, E-cigarette, *E-liquid*, or liquid nicotine, in any facility, in any school vehicle or anywhere on school grounds maintained by the District.

Initial responsibility for enforcement of this prohibition shall rest with building principals, or their designees. Any employee(s) who violate(s) this policy is subject to disciplinary action which may include warning, suspension or dismissal. Violations may also be referred to appropriate law enforcement and/or other appropriate agencies for criminal or other proceedings as provided under state law.

D. All other persons

No visitor, contractor, vendor or other member of the public, shall use any tobacco product, *device*, E-cigarette, *E-liquid*, or liquid nicotine in any facility, in any school vehicle, or anywhere on school grounds maintained by the District.

The building principal(s), and where appropriate, other site supervisor (athletic director, vehicle driver, etc.), or their designee(s), shall have the initial responsibility to enforce this section, by requesting that any person who is violating this policy to immediately cease the use of tobacco products, E-cigarette or liquid nicotine. After this request is made, if any person refuses to refrain from using such products in violation of this policy, the principal, site supervisor, or designee may call contact the appropriate law enforcement agency(ies) for possible criminal or other

Timberlane Regional School District	Policy Code: ADC
Adopted: 07-21-83 Revised: 02-15-99 Revised: 09-11-02 Revised: 02-24-05 Reaffirmed: 11-15-12 Revised: 06-02-16 Revised:	Page 3 of 3

proceedings as provided under state law.

E. Implementation and Notice - Administrative Rules and Procedures.

The Superintendent shall establish administrative rules and procedures to implement this policy, which rules and procedures may be building level and/or district-wide. Rules and procedures relating to student violations and resulting disciplinary consequences should be developed in consultation with building principal(s).

The Superintendent, working with the building principal(s), shall provide annual notice to employees, students and parents of the pertinent provisions of this policy (e.g., student or staff handbook) along with applicable administrative regulations and procedures, which may include prescribed consequences for violations of this policy. Such notice should include information that violation of this Policy could lead to criminal or other such proceedings.

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

Timberlane Regional School District	Policy Code: IHCA
Adopted: 07-21-99 Revised: 04-03-08 Revised: 05-02-13 Revised: 12-19-13 Revised: 06-07-18 Revised:	Page 1 of 1

SUMMER LEARNING

The Board recognizes that student learning is an ongoing process and that it is important for students to engage in learning activities even when not attending school. Therefore, the Board encourages administration to have a plan for summer activities that support student learning. Such activities may include a summer book reading list, attending an education-themed summer camp, engaging in extended learning opportunities, or other activities that support student learning.

School Board Goals

ACADEMICS

1. Develop or improve career pathways for students by extending learning opportunities, negotiating more vocational experiences, expanding dual enrollment possibilities, and non-traditional courses.
2. Establish a career day with the intent to provide a comprehensive summary of all opportunities and pathways for students.
3. Address identified needs for PreK-12 resulting from the prior school year's remote learning by implementing suggestions for improvement within the 2022-23 school year. Identified needs should be determined by June 30, 2022. Create and provide services to address those needs. Support district personnel in addressing those needs.
4. Identify needs for PreK-12 STEAM opportunities to be expanded in the district prior to budget development, with the intent to implement those opportunities into the 2022-23 school year. Establish an event to allow the community to explore and identify the various domains of STEAM.
5. Review data on preparedness for college, workplace, and career, and on success post college gathered via survey for TRSD line of STEAM resources and materials available in classrooms with an explanation of utilization by staff by June 30, 2022.

ADMINISTRATION

1. Evaluate & assess the performance of the SAU in terms of staffing, operation, budget, and organization (as needed).
2. Develop job descriptions for all positions and organizational charts for each department/section etc. by utilizing job descriptions from nearby school districts or determined by the needs of our district. Descriptions must include qualities that could be evaluated at least annually per school year.
3. Identify a comparison group of New Hampshire School districts and use the individual district and aggregate data as metrics to gauge TRSD's student academic achievement and academic growth patterns.
4. Support curriculum work done K-5 to align instruction, assessment, and reporting and to build consistency between elementary buildings.
5. Develop and implement an evaluation system for administrators for annual evaluation prior to contract renewal.

FINANCIAL

1. Evaluate the current budget and look at how to best allocate funds to address any concerns/gaps identified in above academic goal.
2. Audit for TRSD to be free of significant deficiencies and material weaknesses, and to the Board no later than February 2023
3. Ensure the pay structure is equitable and competitive so that we can attract and retain high performing staff.

FACILITIES

1. Remove modular classes from behind PAC, convert to storage containers, and increase parking.
2. Develop a comprehensive Preventative Maintenance Schedule for district equipment, including but not limited to vehicles, tools, power equipment, heating & air conditioning units, etc.
3. Review every school building to determine if each school is adequately meeting the needs of students and staff, with consideration of current learning practices, including STEAM. School adequacy should also be evaluated based on an appropriate student to teacher ratio per classroom determined by the board, based on research and state regulated recommendations.

School Board Goals

BUDGET

1. Receive first draft of CFO's proposed/recommended Operating Budget for FY22-23 with an executive summary for any major budget drivers by October 1, 2022.
2. Receive first draft of CFO's proposed Default Budget for FY22-23 and be provided explanations of justifications for any increases or decreases by line item as is required by statute.

CULTURE CLIMATE

1. Work with the superintendent to incorporate aspects of the current strategic plan (2018-2023) to address identified issues into district schools.
2. Develop a new five-year strategic plan (2024-2029) by January 1, 2023, with a draft developed by October 1, 2022 (in conjunction with the proposed 2022-23 operating budget).
3. Take action when possible to address needs identified in the development of the draft of the five-year strategic plan (2024-2029).
4. Finalize and approve a five-year strategic plan (2024-2029) for implementation by March 1, 2023.
5. Evaluate the prior implementation of the No Bullying initiative and determine if it should be reinstated. If it is determined to be an insufficient solution, determine a different initiative that will incorporate the social-emotional needs of students to more effectively address student behavior instead of relying on punitive discipline.
6. Ensure timely and clear communication to the community regarding district decisions and situations.
7. Support a consistent initiative for collegial feedback and inter building collaboration throughout the district.

Submitted to School Board on June 2, 2022
Steven Finnegan, Chair
Kristin Savage, Vice Chair
Timberlane Regional School Board