Oyster River Cooperative School District
REGULAR MEETING

June 19, 2019 — **High School - Library** — **7:00 PM**

0. CALL TO ORDER (7:00 PM)

I. 6:30 – 7:00 PM MANIFEST REVIEW AT EACH SCHOOL BOARD MEETING.

II. APPROVAL OF AGENDA

III. PUBLIC COMMENTS

IV. APPROVAL OF MINUTES

- Motion to approve 06/05/19 regular meeting minutes.

V. ANNOUNCEMENTS, COMMENDATIONS AND COMMENTS

A. District

B. Board

VI. DISTRICT REPORTS

A. Assistant Superintendent/Curriculum & Instruction Report(s)

- World Language Update – Todd Allen/Jay Richard

B. Superintendent's Report

- Architect Report – Safety
- Charge for MS Grading System
- Request for Student Moving to Newmarket to remain for Senior Year.
- Acknowledgement of 2019 Retirees

C. Business Administrator

- Copier Lease
- Purchase of Transit Vans Approval Lease
- Budget Update FY19

D. Student Senate Report

E. Other:

VII. DISCUSSION ITEM

- Communication Plan

VIII. ACTIONS

A. Superintendent Actions

B. Board Action Item

- Motion to authorize the Superintendent to offer contracts to qualified teachers and staff during the summer months.
- Motion to approve ORHS Speech Pathologist.
- Motion to approve Charge for MS Grading System.
- Motion to authorize Newmarket Student to remain for Senior Year.
- Motion to approve Data Governance Plan for second read/approval.
- Motion to approve Copier Lease.
- Motion to approve Transit Vans Approval Lease.
- Motion to approve Communication Plan.
- Motion to approve List of Policies for first read: KF - Facilities Use, IJL – Library and Instructional Materials Selection and Reconsideration Policy.

IX. SCHOOL BOARD COMMITTEE UPDATES

A. Manifest Reviewed and Approved by Manifest Subcommittee.

X. PUBLIC COMMENTS

XI. CLOSING ACTIONS

A. Future meeting dates: 07/10/19 – Regular Meeting – ORHS Library – 7:00 PM
07/24/19 – Manifest Meeting – SAU Conference RM – 3:30 PM

XII. NON-PUBLIC SESSION: RSA 91-A:3 II (a) {If Needed}

- Personnel Matter

NON-MEETING SESSION: RSA 91-A:2 I {If Needed}

XIII. ADJOURNMENT:

If you require special communication aids, please notify us 48 hours in advance.

The School Board reserves the right to take action on any item on the agenda.

Respectfully submitted,
Superintendent

Oyster River Cooperative School District
SAU #5

Welcome to the School Board meeting. If you wish to be heard by the Board, please note "Public Comment" at the beginning of the agenda (reverse side). During the comment section of the agenda each speaker may have up to three (3) minutes within the time frame allowed. Board Chair may limit time allotment as deemed necessary. Occasionally, the Board may "suspend its rules" to allow visitor participation at the time an issue of specific interest is being addressed. A speaker will not be recognized for a second time on a particular topic.

Visitors should not expect a Board response to their comments or questions under the above since the Board may not have discussed or taken a position on the matter. The Superintendent, without speaking for the Board, may offer clarification as appropriate.

Agendas and background information are available on the district website prior to meetings. Agendas and additional information are generally available at the entrance to the meeting room or distributed at the time the item is introduced for discussion.

The ORCSD School Board will meet in regular session on the first and third Wednesdays of the month with special meetings when necessary. The School Board appreciates your attendance at these meetings and invites your continued interest in its work on behalf of the children and residents of the District.

Oyster River Cooperative School District Members:

• Brian Cisneros	Term on Board: 2018 –2021
• Thomas Newkirk	Term on Board: 2019 - 2022
• Kenneth Rotner	Term on Board: 2019 - 2022
• Denise Day	Term on Board: 2017 - 2020
• Michael Williams	Term on Board: 2017 - 2020
• Allan Howland	Term on Board: 2018 - 2021
• Daniel Klein	Term on Board: 2018 - 2021

Information Regarding Nonpublic Session

On occasion, the Board agenda may include (or be adjusted to include) a Nonpublic Session. When a motion is made to do so, it will be done under the provisions of the NH State Law RSA 91-A:3 II, and one or more of the following reasons will be claimed for entering Nonpublic Session:

a. The dismissal, promotion or compensation of any public employee or the disciplining of such employee, or the investigation of any charges against him, unless the employee affected (1) has a right to a meeting and (2) requests that the meeting be open, in which case the request will be granted.

b. The hiring of any person as a public employee.

c. Matters which, if discussed in public, would likely affect adversely the reputation of any person, other than a member of the public body itself, unless such person requests an open meeting.

d. Consideration of the acquisition, sale or lease of real property or personal property which, if discussed in public, would likely benefit a party or parties whose interests are adverse to those of the general community.

e. Consideration or negotiation of pending claims or litigation which has been threatened in writing or filed against the body or agency of any sub-division thereof, or against any member thereof because of his membership in such body or agency, until the claim or litigation has been fully adjudicated or otherwise settled.

Oyster River Cooperative School District
Regular Meeting
June 5, 2019 **Moharimet School** **DRAFT**

SCHOOL BOARD: Brian Cisneros, Dan Klein, Michael Williams, Al Howland, Denise Day, Kenny Rotner, Tom Newkirk
Not Present: Student Representative: Yasmeen Gunandar

ADMINISTRATORS: Todd Allen, Jay Richard, Suzanne Filippone, Carrie Vaich, Misty Lowe

There were 12 members of the public present.

I. CALL TO ORDER:
6:30-7:00 Manifest Review

II. APPROVAL OF AGENDA:

Move the China Trip Highlights to beginning of the meeting.
There will be two non-meetings but no non-public meeting.
Denise Day moved to approve agenda with the above revisions, 2nd by Brian Cisneros. Motion passed 7-0.

China Trip Highlights: Dave Ervin reported that in April, 52 Oyster River students went on a trip to China. They performed in Beijing and everywhere they performed, they received standing ovations. This trip was very successful and a true cultural exchange. They look forward to further collaborations in the future. Also, a group of students that went on the trip performed at the meeting.

III. PUBLIC COMMENTS:

William Hall from Durham is very impressed with the architectural engineer and that they used borings. He mentioned that the windows of this building should not be able to open from an energy perspective.

Loren Selig of Durham mentioned that her 8th grader has joined the Jazz Band this year and has helped tremendously. She commended Mr. Grove for his reenactment day of the Civil War and is heartbroken that he will not be teaching eighth grade after this year. Lauren is concerned about the disruption of Middle School Teacher changes for next year and the students are very

anxious about this. There is a lot of misunderstanding about the difference between competency-based grading and competency based education.

IV. APPROVAL OF MINUTES:

Motion to approve 05/15/19 regular and non-public meeting minutes
Revision Page 8 Paragraph 4 insert "high school" before CBE
Denise Day moved to approve the 5/15 minutes with the above revision, 2nd by Dan Klein. Motion passed 7-0.

Denise Day moved to approve the non-public meeting minutes, 2nd by Al Howland. Motion passed 7-0.

V. ANNOUNCEMENTS, COMMENDATIONS and COMMENTS:

A. District: Suzanne Filippone, principal of the high school, reminded everyone that graduation is this Friday evening.
David Goldsmith, Principal of Moharimet, reported that the foundations have been poured, the steel is up, and the construction is really starting to take shape. The crews have been really great in educating the students. This spring a logo committee was created consisting of staff and parents and they have already met about six times.

Carrie Vaich of Mast Way stated that this year the culture club has been studying one continent a month. Also, tonight was the annual art show and tomorrow is the senior walk. Our coming week is loaded with activities.

B. Board:

Denise Day has gotten to several various events that are happening in the District. She attended the Action Research Presentations which is the culmination of Chris Hall's Sabbatical this year. She attended the three days of presentations of the teachers and was amazed at the work of the teachers that participated in it.

Al Howland attended the flex time session with Jon Bromley's group. It was a really interesting conversation, it's the beginning and will be coming forward in the fall.

Brian Cisneros also attended the Mast Way Art Show. Deb Hastings did a great job in putting this together.

VI. DISTRICT REPORTS:

A. Assistant Superintendent/Curriculum and Instruction Report

Todd Allen mentioned that Chris Hall's Action Research Presentation is very teacher driven. The teacher summer proposals were awesome this year and 500 teacher days are going to be used this summer. The REACH Program is going to be very busy this summer and will be an incredible program.

Kenny Rotner would like to see Teacher Recognitions Awards in each building. The work that is being done in the schools is phenomenal and they should be formally recognized, and he would like to see this put into place.

B. Superintendent's Report:

Superintendent Morse wanted to thank Carrie Vaich for her professionalism in her transition. There were two teachers and one administration that applied for the interim position. Misty Lowe is the nominee for the transition position.

Superintendent Morse has done fifteen presentations to date on the Middle School project. The reception on the new middle school has been very positive to date.

Josh Olstad has done an amazing job on the Data Governance Plan trying to get NH Schools working together.

Josh reported the details of the plan:
Governance Plan:
As a requirement of RSA 189:66 V every school district needs to develop a data and privacy governance plan. The plan needs to be presented to the school board for review and approval annually. This plan covers the following:

Data Acquisition and creation
Data Management and storage
Data security and protection

Data usage and Dissemination
Data Archiving and Destruction
Disaster Recovery
Data Breach Response
Inventory of Applications Used Across the District

This is work done by schools across the state and uses best practices to meet New Hampshire and federal law. This document is living, and changes made will be presented to the School Board annually for review. The list of applications used across the district will be updated frequently. The action items in this document will take approximately two to three years to fully implement.

Denise Day moved to approve the Data Governance Plan as a first reading, 2nd by Brian Cisneros. Motion passed 7-0.

9th Grade Computer Lease:
Josh Olstead reported on the 9th grade computer lease. They will be leasing 230 Dell Laptops. This is a four year lease for $427.54 each totaling $98,334.20 with a $1 buyout at the end.

Al Howland moved to approve the Dell Computer Lease for $98,334.20, 2nd by Brian Cisneros. Motion passed 7-0.

Josh also reviewed the updates he made to the proposed middle school project on the Oyster River website. This project took 36 hours to complete.

Introduction to Possible Communication Goal:

2019-2020 ORCSD School Board Communications Goal and Actions (Proposed)
The District will take concrete steps to improve communication with parents and Oyster River residents, including improved digital presence and investment in digital communication expertise.

Short Term/Immediate Action:
Launch proposed middle school design website;
Consolidate publication requests;
Review all orcsd.org website content to eliminate obsolete materials and broken links;

Provide everybody who creates content for mass email distribution training on effective email design.

2019-2020 School Year Actions:
Create School Board Blog;
Add a digital communication specialist: approximately 50% time position;
Competency Board education overview;
Social Media Input;
Board Level Public Information;
Develop an acceptable content policy;
Develop social media presence strategy;
Improve mobile version of orcsd.org;
Evaluate communication effectiveness

Denise Day has hesitancy in adding a position with the financial impact and asked whether a proposed position could be a two day position instead.
Tom Newkirk suggested using a consultant to delve into the communication in the District to determine our needs.

Al Howland feels that the competency based information needs to be very clear and how do we get moving forward. This needs to be a focal point if we are going to look at competency-based education.

Michael Williams feels that we need a part time specialist to get this work done in the District.

Kenny Rotner emphasized that we need to improve on how we communicate with the public. We need to be able to reach out to the community.

Al Howland suggested using the tech integrators that we have already hired. Superintendent Morse noted that the tech integrators were hired to be used in the schools and they are out straight with work. He thinks that the communication goal that he has presented is great, but it needs a staff member to make it run. He would have liked to see a full time person. This will be on the agenda for the next meeting.

C. Business Administrator: None
D. Student Senate Report: None
E. Other: None

VII. DISCUSSION ITEM:

Strategic Plan High School Competencies: Revisions

Proposal for Year One Goal: High School Competency Based Education:
Goal: The high school staff and administration will continue work on competency-based education, including the review and posting of competencies. In addition, there will be in-depth discussions with the Board and community about the principles, methods, and direction of this CBE work. These discussions will form a foundation for the delineation of future goals. Years 2-5 will not be filled in.

Tom Newkirk feels that once they start working on this competency-based education work, they will be able to fill in the future years. Michael Williams feels we need to look at how this affects college admissions and how it bridges the middle school and high school, how its communicated with parents and students. We also need to look at what other schools are experiencing.

Superintendent Morse would like to see a little more structure and what the process will be, and how we will explore this. He thinks that the Board should be in a workshop each year with principals and have the dialogue on what the action should be in a given year. Al Howland feels that there seems to be a fragmentation between the middle school and the high school, and they aren't meshing together.

Tom Newkirk moved to approve the above Strategic Plan HS Competencies revisions, 2nd by Brian Cisneros. Motion passed 6-1 with Michel Williams opposing.

School Board Master Schedule: Brian Cisneros moved to approve the School Board Master Schedule, 2nd by Denise Day. Motion passed 7-0.

Superintendent Morse and Sue Caswell presented the Middle School Bond Options:
Common Characteristics:
Can we stage the bond and meet operational budget goals to meet full bond by 2023-24?

Can we commit to 1% growth CIP/Bond in operating budget through 2023-24 and not exceed 3.5% total growth?

Can we delay principal payment and pay three years interest only?

Four Options: All options meet the desired goals.

They:
Meet the goal of affordability
Impact the total budget by $500K a year
Provide the School Board a choice: level debt or level principal
Provide the option of bonding all $49 million at once or divide the bond into 2 issues of $24.5 M

Option 1
$49 Million bond/25 years at 4.25%. No principal payment for two years, interest only.

Year 1: Community engagement March 2020 vote
Plan Design June 2020 Bond Sale
Year 2: Construction Underway Interest only payment
Year 3: Construction Complete Interest only
Year 4: Middle School Bond starts interest only
Year 5: Full Middle School Payment Full interest and principal

Option 2
2 Issues 24.5 M 24.5 M
Year 1: Community engagement March 2020 Plan Design Vote June 2020 Bond Sale
Year 2: Construction Underway sell issue 1 @ 24M Interest only
Year 3: Construction Complete March 2020 Sell Issue 2 @ 24M Interest only
Year 4: Middle School Bond starts Interest
Year 5: HS Bond funds offset CIP Interest and partial principal
Year 6: Full payment interest and principal

Option 3:
2 Issues 24.5M 24.5 M Principal/no payment 2 years
Year 1: Community engagement March 2020 Plan Design Vote 2020 Bond Sale
Year 2: Construction Underway Sell Issue 1 @ 24M Interest only payment

Year 3: Sell Issue 2 @24M Interest Only
Year 4: Middle School Bond starts Interest
Year 5: Interest and partial principal
Year 5: Full Payment Interest and Principal

Option 4:
$49M all at once
Principal for 2 years

Year 1: Community engagement March 2020 Plan Design Vote June 2020 Bond Sale
Year 2: Construction underway Interest only
Year 3: Middle School Bond Starts Interest only
Year 4: Middle School Bond starts interest only

Year 5: Full MS Payment interest and principal
Year 6: Full Middle School Payment Interest and Principal

Superintendent Morse noted that this work is intended for discussion only and he expects that the Board will have multiple discussions and adjustments as they move forward. The final decision by the School Board will need to be made next fall. Once the decision is finalized, they will prepare a warrant for the voters to act on for February 2020 Deliberative Session and for the voters in March 2020.

VIII. ACTIONS:

A. Superintendent Action Items: None
B. Board Action Items:

Motion to List of New Hires:
Denise Day moved to hire the following list of new hires in the District:
Misty Lowe
Lauren Gray
Daniel Chick
Kimberly Felch
Emily Varnese
Kayla Livingston
Jane "Kyra" Dulmage
Patricia VanDeventer

2nd by Brian Cisneros. Motion passed 7-0.

Motion to approve ORHS Fall 2019 Coach:
Denise Day moved to approve Cydney Scarano Girls Varsity Head Soccer $4,175 2nd by Brian Cisneros. Motion passed 7-0.

Motion to approve List of Policies for second reading/adoption:
EHAB Data Governance and Security

Denise Day moved to approve Policy EHAB for second reading, 2nd by Brian Cisneros. Motion passed 7-0.

IX. SCHOOL BOARD COMMITTEE UPDATES:

A. Manifest Reviewed and Approved by Manifest Committee:
Denise Day reported that the Manifest Committee met both last week and this evening.

Payroll Manifest #23: $963,855.60
#24: $1,481,729.47
Vendor Manifest: #27: $97,125.42

Middle School Building Committee: Tom Newkirk reported that the administrative offices will not be moving into the proposed middle school.

X. PUBLIC COMMENTS:

Stephanie Griffin of Durham talked about the communication discussion and strongly encouraged the Board to have an opt in email list to receive School Board minutes and the agenda.

Loren Selig of Durham mentioned that the kids at the middle school don't understand the grading system and encouraged the Board to talk to the students and parents moving forward.

Michelle Marstinson of Lee was disappointed in the grading system when they moved here and doesn't feel that the kids have anything to strive for.

XI. CLOSING ACTIONS:

A. **Future Meeting Dates:** June 19th Regular Meeting ORHS Library 7:00 p.m.

XII NON-PUBLIC SESSION RSA 91-A:3 II c

NON-MEETING SESSION: RSA 91-A:2 I b

- Strategy or negotiations with Respect to Collective Bargaining

XIII. ADJOURNMENT:

The School Board entered a non-meeting session that ended at 9:50 p.m. to discuss negotiations for collective bargaining, returned to public session, and entered a second non-meeting which ended at 10:18 PM. **Al Howland made a motion to adjourn at 10:19 PM, seconded by Brian Cisneros.**

Respectfully yours,
Laura Grasso Dobson
Recording Secretary

Office of the Superintendent
Oyster River School District
36 Coe Drive, Durham, NH 03824

INTEROFFICE MEMORANDUM

TO: School Board
FROM: Todd Allen, Asst. Superintendent
Jay Richard, Principal ORMS
DATE: June 19, 2019

RE: ORCSD World Language Committee Progress Report

In January 2019 the OR School Board authorized the creation of a committee to examine the World Language program in the school district. The committee was asked to make recommendations on the possibility of adding a K-5 program. The committee was given the following charge by the OR School Board.

"To investigate current research related to effective elementary world language programs, to identify the obstacles faced including how world language would fit into the schedule and to present best practice options with a preliminary report in May, with a final report in September 2019 for Board consideration."

The charge was later modified to make the due date for the final report in November 2019.

Committee Members:
Leslie Ayers, World Language Teacher at ORHS
Candace French, World Language Teacher at ORMS
Kate Zimar, Classroom Teacher at Mast Way
Andrea Birkel, Moharimet parent and OR community member
Kristin Laberis, Moharimet parent and OR community member
Anita Mathur, Mast Way parent and OR community member
David Goldsmith, Principal of Moharimet
Carrie Vaich, Principal of Mast Way
Jay Richard, Principal of ORMS
Todd Allen, Assistant Superintendent

Progress to date:

- The committee has met regularly starting in February 2019
- The committee has reviewed a wide range of research
  - Brown University Guide to starting a WL program
  - Middlebury Interactive Language research
  - A variety of policy papers and research
- Developed a community survey about K-4 World Language options
- Reviewed master schedules at MW, MOH and ORMS as well as multiple other schools with K-4 World language programs
- Two school visits have been conducted to Rye, NH and Keene, NH
- Wayland and Brookline school districts have been contacted.
- Additional visits are planned in the fall to Glastonbury, Ct, Dover-Sherborn, Ma, Newington, NH and others as identified by the committee.

Plan for 5th Grade students taking Chinese in 2019-20:

For 2019-20 there are ten 5th grade students who will be continuing with Chinese study at ORMS. In order to accommodate this need Principal Richard has worked with the families of these students to determine the best manner of scheduling the experience. The plan for the fall of 2019 is to schedule Chinese instruction in 5th grade 3 times a week during Bobcat Time starting on October 1st. By doing it this way, the students are given the first month of school to transition to a new school and can access supports in other subject areas 2 days a week.

Draft of k-4 World Language Survey (Edited 4-5-19)

The Oyster River Cooperative School District is investigating options for world language study at the k-4 level. The OR School Board has asked Superintendent Morse to form a committee made up teachers, parents and administration to research best practices in world language instruction and make recommendations in the fall of 2019. The specific charge of the committee is as follows:

"To investigate current research related to effective elementary world language programs, to identify the obstacles faced including how world language would fit into the schedule and to present best practice options with a preliminary report in May, with a final report in September 2019 for Board consideration.

In the interest of identifying the best path forward for world language instruction in the ORCSD please respond to the following questions.

Would you support a world language program for grades k-4 taking place during the school day?

Yes, no, no preference

Comments:

Would you support a school sponsored model of world language study that occurred after school or extended the school day for those who participated?

Yes, no, no preference

Comments:

Currently there are three languages being offered to students in the ORCSD (French, Spanish and Chinese) in grades 6-12. If only one language were to be offered at the k-4 level which one should it be?

French, Spanish, Chinese, no preference

Comments:

Please rate these options for world language study by your personal preference on a scale of 1 to 5 with 5 being highly desirable.

French
Spanish
Chinese

Depending on the outcome that a world language program hopes to achieve the focus of the program will vary.

What should the primary goal of a k-4 world language program be?

1. Increasing fluency in a target language: With this focus students need to be exposed to 25-30 minutes for 3 times per week.
2. Exposure to diverse cultures: With this focus curriculum is integrated and can occur as often as is desired.
3. An introduction to world language study: With this focus students should be exposed to at least one period per week of 30-45 minutes.

Comments:

Use the space below to share any additional input that you would like the World Language Committee to consider in making its recommendation to the Oyster River School Board.

Comments:

Office of the Superintendent
Oyster River School District
36 Coe Drive, Durham, NH 03824

INTEROFFICE MEMORANDUM

TO: School Board
FROM: Dr. James C. Morse, Sr.
DATE: June 19, 2019

RE: Architect Report – Safety

Safety/Security

- Floor Plan
- Site Plan

Resources

As we know, the current middle school has many safety concerns.

Outside Safety Concerns:

Due to the traffic pattern students are intermingling with traffic which is dangerous. Our current building has multiple entrances which makes it that much more difficult to monitor. In addition, cars and buses are constantly jockeying for position, never a good thing when discharging students.

Inside Safety Concerns:

The current middle school also has inside safety concerns.

There are multiple points of entry to the building that make managing outside visitors to the school challenging. There are many ground level windows that are not safety glass in front and back of the building. Access to the building is challenging due to handicap accessibility issues. Due to the sprawling nature of the building there is poor corridor visibility throughout the building. Air quality is poor due to inadequate ventilation.

Architect Lamarre will share how the conceptual designs of the proposed middle school will address safety concerns. Ron will present to the School Board how his design incorporates safety as one of the primary design elements to ensure our students and staff have a safe, healthy and welcoming environment.

The Board charges the Superintendent to create a committee to assess the effectiveness of the current middle school progress reporting system – and, if necessary, to make recommendations for changes. The committee should be composed of parents, teachers, and students. Using survey and focus group tools, the committee will seek out the views of students, parents, and teachers on issues that include, but are not limited to:

- The clarity and precision of the system.
- The effect of the system on student motivation.
- The transition from middle school system to the high school system.

The committee will complete its work in the Fall of 2019-20 and have a report to the Board by May 2020. The Board will support the use of the current budget in regards to this.

Approved ORCSD Board: _____

Office of the Superintendent
Oyster River School District
36 Coe Drive, Durham, NH 03824

INTEROFFICE MEMORANDUM

TO: School Board
FROM: Dr. James C. Morse, Sr.
DATE: June 14, 2019

RE: 2018 - 2019 Retirees

2018 – 19 Retirees			
School/Position	**Last**	**First**	**Years of Service**
High School/Custodian	Byron	Paul	19
" SpEd Paraprofessional	Kester	Barbara	5
Middle School/Language Arts	Rief	Linda	38
" " "/School Nurse	Moran	Eileen	23
" " "/Speech/Lang	O'Brien	Janice	21
" " /Paraprofessional	Mahokin	Pamela	21
" " "/Special Ed	Grout	Alexa	15
Mast Way/Counselor	Tirrell	Brenda	17
SAU/Facilities			
SAU/ Accounts Payable	Paradis	June	31
Facilities/Secretary	Poulin	Deb	21

Office of the Superintendent
Oyster River School District
36 Coe Drive, Durham, NH 03824

INTEROFFICE MEMORANDUM

TO: School Board

FROM: Sue Caswell,
Business Administrator

DATE: June 19, 2019

RE: Copier Lease

We are coming to the end of our lease on the copiers/printers in the district. The new proposal we are recommending is with Canon for 39 devices: 24 copiers and 15 printers, maintenance and supplies. As a member of National IPA we are using their Prebid contract for this lease. It would be a 5-year lease with no increases on per copy costs. Josh has met with each of the principals and reviewed their needs to right size the machines in each building.

Since this is a lease agreement it requires the approval of the School Board.
Josh Olstad, Technology Director, is available to answer any questions you may have.

We need a motion to approve entering a 5 year lease with Canon Solutions of America for copiers and printers.

Oyster River Cooperative School District
Business Administrator's Office

SAU # 5
36 Coe Drive
Durham, NH 03824

(603) 868-5100 x2003
FAX (603) 868-6668
scaswell@orcsd.org

INTEROFFICE MEMORANDUM

TO: School Board

FROM: Sue Caswell,
Business Administrator

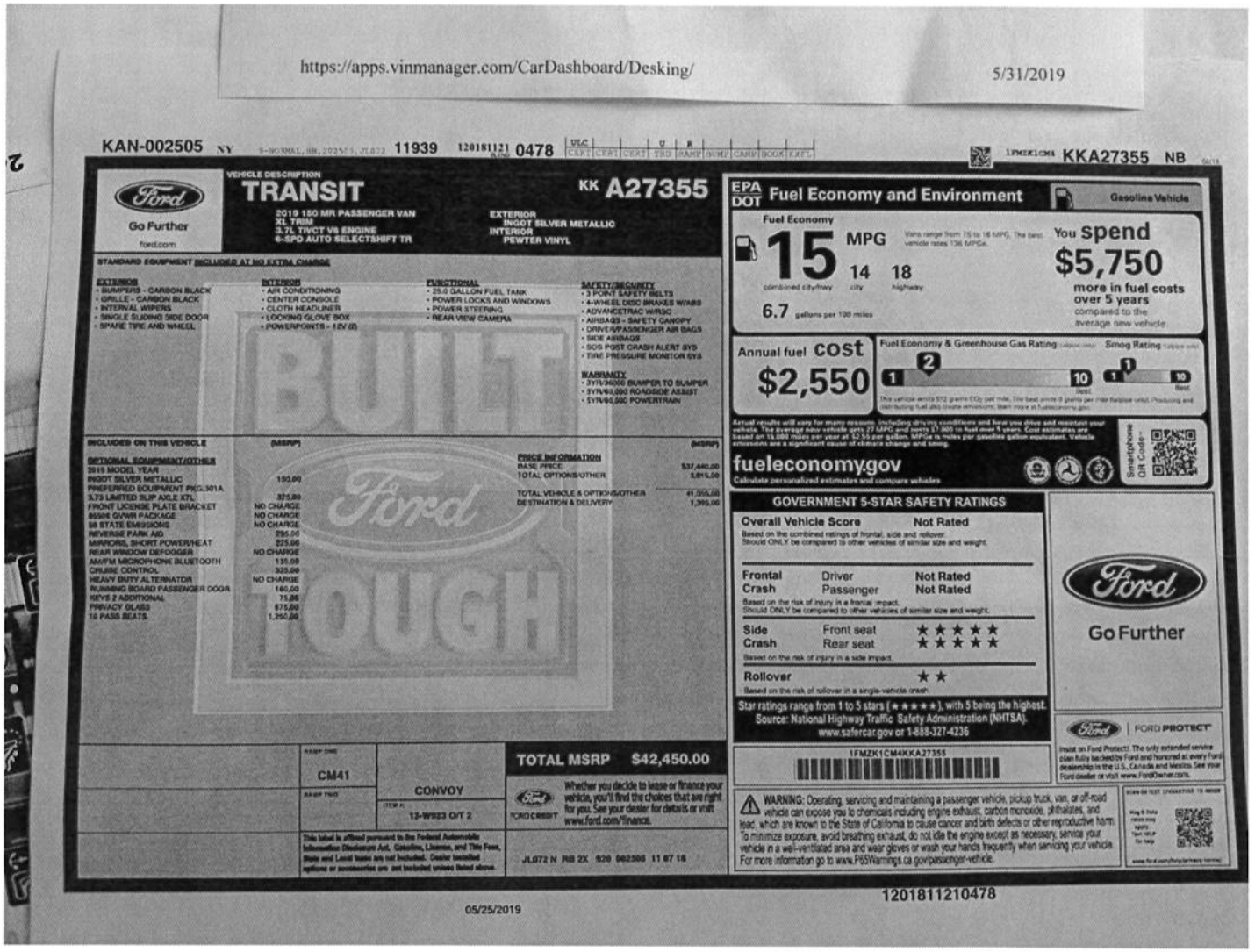
DATE: June 19, 2019

RE: Van Replacement

The increase in the need for specialized transportation has made it difficult to cover the needs of the district. We now have only 3, 6-passenger vans providing this coverage. They are all 2013 vehicles with high mileage and repairs are beginning to get expensive. With only 3 vans available we have some of our 77 passenger buses transporting just 6-8 students on some routes.

We have funds in the budget to replace 2 vans. Lisa Huppe has contacted several dealers in the area and would like to purchase 4, 10-passenger Ford Transits Vans from Bill Dube. With a $20,000 down payment from this year's budget and the funds in next year's budget we could cover a 4-year payment plan on 4 of these vehicles. This option would allow us to move more students with less vehicles.

We need a motion to approve the financing to purchase 4, Ford Transits Vans utilizing $20,000 from the 2018-19 budget for a down payment.



https://apps.vinmanager.com/CarDashboard/Desking/ 5/31/2019

KAN-002505 NY 11939 1201811210478 0478 KKA27355 NB

Ford Go Further ford.com

VEHICLE DESCRIPTION
TRANSIT
2019 150 MR PASSENGER VAN
XL TRIM
3.7L TIVCT V6 ENGINE
6-SPD AUTO SELECTSHIFT TR

KK A27355

EXTERIOR
INGOT SILVER METALLIC
INTERIOR
PEWTER VINYL

STANDARD EQUIPMENT INCLUDED AT NO EXTRA CHARGE

EXTERIOR
- BUMPERS - CARBON BLACK
- GRILLE - CARBON BLACK
- INTERVAL WIPERS
- SINGLE SLIDING SIDE DOOR
- SPARE TIRE AND WHEEL

INTERIOR
- AIR CONDITIONING
- CENTER CONSOLE
- CLOTH HEADLINER
- LOCKING GLOVE BOX
- POWERPOINTS - 12V (2)

FUNCTIONAL
- 25.0 GALLON FUEL TANK
- POWER LOCKS AND WINDOWS
- POWER STEERING
- REAR VIEW CAMERA

SAFETY/SECURITY
- 3 POINT SAFETY BELTS
- 4-WHEEL DISC BRAKES W/ABS
- ADVANCETRAC W/RSC
- AIRBAGS - SAFETY CANOPY
- DRIVE/PASSENGER AIR BAGS
- SIDE AIRBAGS
- SOS POST CRASH ALERT SYS
- TIRE PRESSURE MONITOR SYS

WARRANTY
- 3YR/36000 BUMPER TO BUMPER
- 5YR/60,000 ROADSIDE ASSIST
- 5YR/60,000 POWERTRAIN

BUILT FORD TOUGH

INCLUDES ON THIS VEHICLE	(MSRP)
OPTIONAL EQUIPMENT/OTHER	
2019 MODEL YEAR	
INGOT SILVER METALLIC	150.00
PREFERRED EQUIPMENT PKG.301A	
3.73 LIMITED SLIP AXLE XTL	325.00
FRONT LICENSE PLATE BRACKET	NO CHARGE
850# GVWR PACKAGE	NO CHARGE
50 STATE EMISSIONS	NO CHARGE
REVERSE PARK AID	295.00
MIRRORS, SHORT POWER/HEAT	325.00
REAR WINDOW DEFOGGER	NO CHARGE
AM/FM MICROPHONE BLUETOOTH	135.00
CRUISE CONTROL	325.00
HEAVY DUTY ALTERNATOR	NO CHARGE
RUNNING BOARD PASSENGER DOOR	160.00
KEYS 2 ADDITIONAL	75.00
PRIVACY GLASS	575.00
10 PASS SEATS	1,250.00

PRICE INFORMATION	(MSRP)
BASE PRICE	$37,440.00
TOTAL OPTIONS/OTHER	3,815.00
TOTAL VEHICLE & OPTIONS/OTHER	41,255.00
DESTINATION & DELIVERY	1,195.00

RAMP ONE CM41
RAMP TWO
CONVOY
ITEM A 13-W923 O/T 2

TOTAL MSRP $42,450.00

FORD CREDIT Whether you decide to lease or finance your vehicle, you'll find the choices that are right for you. See your dealer for details or visit www.ford.com/finance.

This label is affixed pursuant to the Federal Automobile Information Disclosure Act. Gasoline, License, and Title Fees, State and Local taxes are not included. Dealer installed options or accessories are not included unless listed above.

JL072 N RB 2X $20 002505 11 07 18

EPA DOT Fuel Economy and Environment — Gasoline Vehicle

Fuel Economy
15 MPG combined city/hwy (14 city, 18 highway)
6.7 gallons per 100 miles

Vans range from 15 to 16 MPG. The best vehicle rates 136 MPGe.

You spend $5,750 more in fuel costs over 5 years compared to the average new vehicle.

Annual fuel cost $2,550

Fuel Economy & Greenhouse Gas Rating (1 worst, 10 best) Smog Rating (1 worst, 10 best)

This vehicle emits 572 grams CO2 per mile. The best emits 0 grams per mile tailpipe only. Producing and distributing fuel also create emissions; learn more at fueleconomy.gov.

Actual results will vary for many reasons, including driving conditions and how you drive and maintain your vehicle. The average new vehicle gets 27 MPG and earns $7,900 in fuel over 5 years. Cost estimates are based on 15,000 miles per year at $2.55 per gallon. MPGe is miles per gasoline gallon equivalent. Vehicle emissions are a significant cause of climate change and smog.

fueleconomy.gov
Calculate personalized estimates and compare vehicles

SmartPhone QR Code

GOVERNMENT 5-STAR SAFETY RATINGS

Overall Vehicle Score: Not Rated
Based on the combined ratings of frontal, side and rollover. Should ONLY be compared to other vehicles of similar size and weight.

Frontal Crash — Driver: Not Rated; Passenger: Not Rated
Based on the risk of injury in a frontal impact. Should ONLY be compared to other vehicles of similar size and weight.

Side Crash — Front seat: ★★★★★; Rear seat: ★★★★★
Based on the risk of injury in a side impact.

Rollover: ★★
Based on the risk of rollover in a single-vehicle crash.

Star ratings range from 1 to 5 stars (★★★★★), with 5 being the highest. Source: National Highway Traffic Safety Administration (NHTSA). www.safercar.gov or 1-888-327-4236

Ford Go Further

1FMZK1CM4KKA27355

Ford FORD PROTECT
Invest on Ford Protect! The only extended service plan fully backed by Ford and honored at every Ford dealership in the U.S., Canada and Mexico. See your Ford dealer or visit www.FordOwner.com.

WARNING: Operating, servicing and maintaining a passenger vehicle, pickup truck, van, or off-road vehicle can expose you to chemicals including engine exhaust, carbon monoxide, phthalates, and lead, which are known to the State of California to cause cancer and birth defects or other reproductive harm. To minimize exposure, avoid breathing exhaust, do not idle the engine except as necessary, service your vehicle in a well-ventilated area and wear gloves or wash your hands frequently when servicing your vehicle. For more information go to www.P65Warnings.ca.gov/passenger-vehicle.

SCAN OR TEXT 1FMZK1CM4KKA27355 TO 88538
Msg & Data rates may apply. Text HELP for help.

05/25/2019 1201811210478

OYSTER RIVER COOPERATIVE SCHOOL DISTRICT
FISCAL YEAR 2018-19
FINANCIAL STATUS AS OF:

6/12/2019

	Budgeted	Expended	Encumbrances	Amount Remaining	Percentage Spent
	2017-2018	2017-2018	2017-2018	2017-2018	2017-2018
SALARIES:					
Administrator	1,479,199	1,418,930	58,916	1,353	100%
Teacher	16,287,558	13,020,039	2,931,800	335,719	98%
Para	2,175,446	1,977,139	111,226	87,081	96%
Tutor	220,677	203,388	10,383	6,906	97%
Custodian	785,237	720,688	30,611	33,938	96%
Secretary	382,576	400,716	25,558	(43,698)	111%
District Hourly	755,296	738,049	27,881	(10,634)	101%
Maintenance	196,754	191,033	9,481	(3,760)	102%
Drivers	805,718	646,670	80,671	78,377	90%
Misc & Summer	179,500	146,748	1,200	31,552	82%
Subs - Professional	358,580	266,681	3,435	88,464	75%
Subs - Para	35,300	37,720	0	(2,420)	107%
Subs - Secretary	6,700	3,809	0	2,891	57%
O/T	25,500	11,697	0	13,803	46%
Med & Dent Payback	474,087	385,195	20,533	68,359	86%
TOTAL SALARIES	**24,168,128**	**20,168,502**	**3,311,695**	**687,931**	**97.2%**
BENEFITS:					
Health Ins	5,242,759	4,192,776	1,141,719	(91,736)	102%
Dental Ins	144,579	114,976	31,053	(1,450)	101%
Life Ins	61,226	50,559	13,743	(3,076)	105%
LTD Ins	64,475	41,904	11,605	10,966	83%
FICA	1,838,023	1,482,837	253,179	102,007	94%
Retirement - Non Professional	336,399	324,441	13,818	(1,860)	101%
Retirement - Professional	2,941,787	2,367,200	511,693	62,894	98%
Annuity	128,134	122,596	14,659	(9,121)	107%
Tuition Reimb	5,000	1,335	0	3,665	
Unemployment Comp	15,000	124	0	14,876	1%
Workers Com	153,108	153,108	0	0	100%
TOTAL BENEFITS	**10,930,490**	**8,851,856**	**1,991,469**	**87,165**	**99.2%**
ALL OTHER OPERATING EXPENSES:					
Mast Way	257,563	169,660	3,009	84,894	67%
Moharimet	177,675	133,970	5,075	38,630	78%
Middle School	362,001	323,866	5,635	32,500	91%
High School	690,687	652,535	16,197	21,955	97%
District	1,973,842	1,982,722	913	(9,793)	100%
Transportation	495,530	525,541	0	(30,011)	106%
Technology	690,778	629,870	4,691	56,217	92%
Facilities	3,010,495	3,437,084	69,802	(496,391)	116%
SPED	1,560,831	1,558,410	146,385	(143,964)	109%
TOTAL OPERATING	**9,219,402**	**9,413,658**	**251,707**	**(445,963)**	**104.8%**
GRAND TOTAL	**44,318,020**	**38,434,016**	**5,554,871**	**329,133**	**99.3%**
Remove state grant covered facilities spending		(572,403)		572,403	
Adjusted totals	44,318,020	37,861,613	5,554,871	901,536	

Comment Section:

2019-2020 ORCSD SB Communications Goal and Actions (Proposed) 30 May 2019

2019-2020 communications goal: The District will take concrete steps to improve communication with parents and Oyster River residents, including improved digital presence and investment in digital communications expertise.

Short Term / Immediate Actions:

1. Launch **proposed middle school design web site,** including concept drawings, presentations where available (i.e. sustainability slides from 15 May board meeting), vote and construction schedule information, future public meeting dates, etc. Completion goal: website launched by June 30, 2019 (preferably sooner).
2. **Consolidate publication requests** to Durham Friday Updates. Establish single point of contact to group content from all schools for requested publication in Durham's Friday Updates to ensure consistent format and grouped content. Completion goal: June 30, 2019. Responsible: Executive Assistant.
3. Review all orcsd.org website content to **eliminate obsolete material and broken links**, on desktop and mobile versions. Remove or refresh any obsolete content. Completion goal: August 20, 2019. Responsible: IT department (broken links), building principals and department heads (content review).
4. Provide everybody who creates content for mass email distribution **training on effective email design** (i.e. minimize number of steps for clicking to additional links to access basic / essential content, selecting appropriate attachment / image format, how much information should be grouped together, archiving information on school web site if appropriate). Complete before August 31, 2019. Responsible: IT team in collaboration with Principals/Department Heads.

2019-2020 School Year Actions:

5. **Create School Board Blog**, a location where board members can publish and archive content for public consumption. The blog can contain a detailed explanation or discussion of an issue, including mixed media, and a short description with link can be distributed to other channels (i.e. school facebook pages, Durham Friday Updates, PTOs) for easy access. Examples of topics to be addressed could include updates on MOH construction, proposed middle school design, strategic plan, world language, budgets, etc. Proposed content could be produced or sponsored by any board member, then reviewed by Superintendent Morse and Chair Newkirk, then published. This requires platform support from IT. If determined feasible, goal is to launch blog by August 31, 2019. Responsible: IT department and School Board.
6. **Add a digital communications specialist** (approx. 50% time position) to provide consistent and responsive community engagement in on-line publishing and social media, support staff development in use of latest communication tools, keep tools and content current, evaluate communication effectiveness, and provide a single-point-of-contact both internally and externally for management of district digital and social media. Begin Recruiting immediately upon approval. Target hiring by October 1, 2019. Responsible: Superintendent.
7. **Competency Based Education Overview:** Compile and publish a parent-friendly overview of K-12 competency-based-education explaining reasons and benefits of CBE, how it is used at ORMS, interaction of CBE with powerschool and report cards, process of discernment for CBE implementation at ORHS, and description of how CBE programs will be evaluated at ORMS and ORHS. It will also address concerns about student motivation, consistency between teachers/subjects, impact on college applications, communication expectations between school and home. Completion goal: October 1, 2019. Responsibility: Assistant Superintendent.

8. **Social media input**: Develop channel for collecting feedback from online conversations *about* the district, even if not addressed to the district directly, from social media sites (i.e. twitter, facebook) and providing feedback to relevant administrators. Review current feedback. Completion goal for developing process: October 31, 2019. Responsible: Digital communications Specialist
9. **Board Level Public Information**: Distribute board meeting Agenda/Backup and Meeting Summary via opt-in mailing list (may contain link directly to files on school website or SB Blog) or similar method. Post board meeting summaries no than 3 days after meeting (Ongoing). Goal: set up distribution list by November 30,2019. Responsibility: Communications Specialist, Executive Assistant, School Board.
10. **Develop an acceptable content policy** for district web sites including the school board blog, to guide content creators in best practices for what should be shared online and at what level of detail. This will also provide a level of objectivity in assessing the appropriateness of published material. Target deliver proposal to Policy Committee by December 15, 2019. Responsible: Digital communications Specialist and Superintendent.
11. **Develop social media presence strategy** by reviewing how UNH, other school districts, etc. use social media and determine which platform(s) the district should use and in what ways. Target completion: January 31, 2020. Responsible: Communication Specialist.
12. **Improve mobile version of orcsd.org** website. Optimize navigation and available content. Timing at discretion of communications specialist. Responsible: Digital communications specialist and IT.
13. **Evaluate communication effectiveness** by following up on selected district communications (i.e. select at least 2 items per month to follow-up on by reviewing content viewing statistics, follow-up targeted email / short survey, or other tools) with target audience to ensure the intended message is received and provide feedback to content creators. Target first evaluation and feedback completed by March 1, 2020. Responsible: Digital communications specialist.

Digital Communications Specialist – overview job description (see action #6)

Your job: As the ORCSD Digital Communications Specialist, you will be a leader in the school district's day-to-day communications with students and their families, residents/taxpayers of the school district, and media. You would serve as the primary point-of-contact for publishing digital media content to the district's web sites and social media, support staff in using media creation and publishing tools, maintain platforms that enable others in the district publish content, develop digital media policy and strategy, provide staff with feedback on online conversations, and evaluate the effectiveness of school communications. You'll make sure that all published material is appropriate for community consumption and complies with district policy and law including student privacy and protection.

Your background: As the ideal candidate, you have demonstrated experience with creating and publishing online content (we want to see your portfolio!), and you've taught or coached others in good online and social media presence. You have extensive knowledge of current social media platforms and you have strong experience in using various software to create different types of content. It's a plus if you have a background in education or experience working in a school environment. You are detail-oriented both when creating your own content and when helping others with theirs. You've brought together multiple stakeholders providing input to a common online identity. You might have formal public/community relations or web design training, but that's not essential. We hope you've worked in this area for at least a year. You solve problems collaboratively and support the district's educational mission.

Oyster River Cooperative School District

Nomination Form

#of Resumes Received: 9

Name:	Alison Richards
Date:	06/13/19
Position:	Speech Pathologist
Person Replacing:	Emily Johnson 1 yr LOA
Budgeted Amount:	$53,100
Recommended Step/Salary:	MA/6 $55,421
Interviewed By:	Andrea Biniszkiewicz, Nellie Dinger, Kim Donovan, Val Wolfson, Laurenne Ramsdell, Juliann Woodbury
# Interviewed:	5
Education:	BA in Communication Science - University of Vermont MA in Speech-Language Pathology - UNH
Certification: HQT Status	CCC-SLP State of New Hampshire #1197
Related Experience:	Newmarket School Department - Newmarket, NH 2007-2009 Clearly Speaking, Dover, NH 2009-Present {Part-Time}
Comments:	Ms. Richards has an extremely professional and collaborative demeanor. She has experience in both the school and clinical setting of speech pathology. Ms. Richards has worked with students aged preschool through high school.
Date: June 13, 2019	Authorized Signature: Andrea Biniszkiewicz

REQUIRED Attachments:

■ Resume ☐ 3 Letters of Recommendation ■ Copy of Certification

Revised 5/7/09, 9/12/11 to include HQT Status, 7/17/15

DATA AND PRIVACY GOVERANCE PLAN

Oyster River Cooperative School District

Table of Contents

DRAFT

DRAFT

DRAFT

Introduction

The Oyster River Cooperative 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 Oyster River Cooperative 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 Oyster River Cooperative 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 Oyster River Cooperative School District's Data Governance team consists of the following positions: Superintendent, Assistant Superintendent, Business Administrator, Director of Special Services and the Director of Technology, System Administrator, and others as necessary. 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 System 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 Oyster River Cooperative 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 that promote the educational objectives of Oyster River Cooperative 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 Oyster River Cooperative 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 and governance 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 Oyster River Cooperative 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 Oyster River Cooperative 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 Oyster River Cooperative School District complies with all 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(link)
- 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 Oyster River Cooperative 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, EHAB (Data Governance and Security – pending school board approval), GBEF (School District Internet Access for Staff), GBEF-R (School District Internet Access for Staff Rules), JICL (Student Computer & Internet Use), JICL-R (Acceptable Internet Use Procedures - Student) 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.

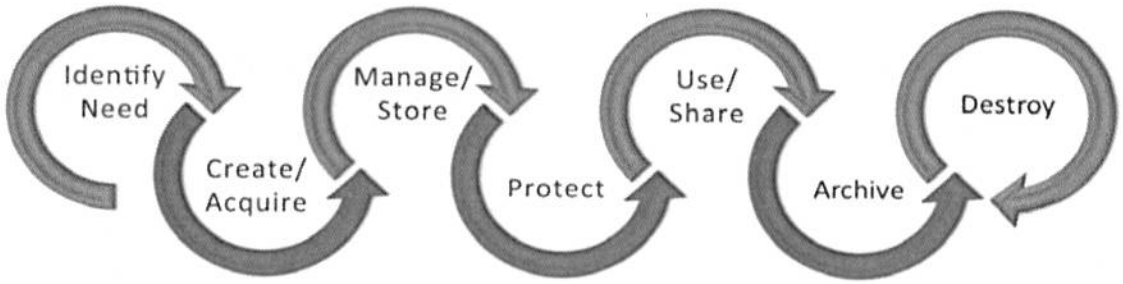
Any attempted violation of district policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.

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.
- 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.

The Oyster River Cooperative School District will establish a process for vetting new digital resources. Staff will be required to complete the process, to ensure that all new resources meet business and/or instructional need as well as security requirements.

Memorandums of understanding (MOU), contracts, terms of use and privacy policy for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the 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:
    - The district continues to own the data shared, and all data must be available to the district upon request.
    - 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.
    - District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
    - The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
    - No API will be implemented without full consent of the district.
    - All data will be treated in accordance to federal, state and local regulations
    - The provider assumes liability and provides appropriate notification in the event of a data breach.

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

A current list of all vetted and approved software systems, tools and applications will be published on the Oyster River Cooperative School Districts website.

Review of Existing Systems

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

Individual student level data is submitted to different approved service providers in order to ensure business operations and instructional services. At times, these imports include PII for staff and student. 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

After completing the requirements for adoption of any new systems, staff shall complete an online request form or any new digital app/tool that either has an associated cost or collects staff or student data (see Appendix C: Digital Resource Acquisition and Use). All staff must adhere to the following guidelines regarding a new digital resource acquisition:

- Contracts for any system that creates, collects or uses personally identifiable information (PII), student records or confidential data must be reviewed by the ISO prior to initiation. Staff should speak with their building Technology Integrator before using ANY new app/online tool with students and seek their assistance with the evaluation/vetting process. This includes any online tool that a student interacts with where they may be creating content and/or any site that requires any student login.

- It is the responsibility of the staff requesting to use new digital content to properly vet the resource to ensure that it meets 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.

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

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 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 listed on 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.

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 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 School District Internet Access for Staff and Students (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 computers and devices will be provided with several options for data storage and transmission. Staff and students will need to ensure that they are securely storing their data. Staff and students will be able to store data on the local device. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. Staff and students will also have a mapped personal folder, known as the Z Drive. Access to these files is restricted to the folder's owner (staff or student who is assigned) and district enterprise administrator accounts.

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 an account that provides unlimited cloud storage. Users are responsible for all digital content in this account (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 containing PII 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 in reviewed and approved by the Superintendent or designee. All other mass downloads of information shall be approved by the ISO and include only the minimum amount of information necessary to fulfill the request.

Printing

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

Oral Communications

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

Training

The 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 irretrievable.

District Data Destruction Processes

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

- Data in an active litigation hold will be maintained until the conclusion of the hold.
- Student accounts will be disabled after the student's final date of attendance. Any files associated with the account will be deleted after one year.
- Staff accounts will be suspended after the final workday, unless HR or the ISO approves a district administrator to maintain access.

Asset Disposal

The district will maintain a process for physical asset disposal. 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 biannually.

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).

DRAFT

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).

DRAFT

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 or update information. A user of data is expected to:

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

DRAFT

Appendix B - Laws, Statutory, and Regulatory Security Requirements

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

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

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

HIPAA: The Health Insurance Portability and Accountability Act applies to organizations that transmit or store Protected Health Information (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

DRAFT

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 for Privacy and Security of Student and Employee Data

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

An online request form will be 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:
    - The district continues to own the data shared, and all data must be available to the district upon request.
    - 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.

- District data will be maintained in a secure manner by applying appropriate technical, physical and administrative safeguards to protect the data.
- The provider will comply with district guidelines for data transfer or destruction when contractual agreement is terminated.
- No API will be implemented without full consent of the district.
- All data will be treated in accordance to federal, state and local regulations
- The provider assumes liability and provides appropriate notification in the event of a data breach.
- Note: Exceptions can be made by the ISO when all the criteria cannot be met for a legitimate reason while still meeting all regulatory requirements for use. Parent permission is requested from parents during the yearly online registration process for 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 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:
  - kept on file in the technology office.
  - accurate, up to date, and adequate.
  - in compliance with all copyright laws and regulations.
  - in compliance with district, state and federal guidelines for data security.
- Software installed on Oyster River Cooperative 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.

DRAFT

Appendix D - Data Security Checklist

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

DRAFT

DRAFT

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
- Participation of students in officially recognized activities and sports
- Grade level
- Height and weight of student athletes
- Dates of attendance in the school district
- Honors and awards received

DRAFT

- Photographs and videos relating to student participation in school activities open to the public

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

Public Information

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

This information may be disclosed outside of the district.

DRAFT

Appendix F - Securing Data at Rest and Transit

All staff and students that log into a district owned 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 school district provided device. The data on the local hard drives of district owned devices is encrypted to ensure its security. It is important to note that this data is not a part of the district's continuity plan, and thus will not be backed up by the district's backup solution. Staff and students will also have a mapped personal folder, known as the Z Drive. Access to these files is restricted to the folder's owner (staff or student who is assigned) and district enterprise administrator accounts.

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

Cloud Storage and File Sharing

The term "Cloud Storage" is used to define all types of remote server storages accessed by users through the Internet. All staff and students are provided an account that provides unlimited cloud storage. Users are responsible for all digital content in this account. When using cloud storage, staff and students must adhere to the following guidelines:

- Staff and students may not access cloud storage through third party applications outside of approved internet browsers and vendor provided applications.
- Users need to be aware of default sharing settings on folders when they upload files. Users are required to limit sharing files to an as needed basis.
- Staff and students must ensure that any cloud storage providers used are approved by the district and meet district student data and data security standards.
- When exiting the district, students should responsibly copy their content to their own personal storage solution.
- When exiting the district, staff should ensure that they are only copying personal content that they created. Staff are prohibited from copying content that contains confidential information, student records or data.
- Data with personally identifiable information of staff or students may be posted to users' district provided Microsoft 365 account with appropriate security settings. Users may not post this data to other cloud sharing platforms without consent of district administration.
- 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 and students have no expectation of privacy on data stored on any district provided platform.

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

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

External Storage Devices

The term "External Storage Devices" is used to define all portable storage devices (including USB drives, rewritable CD/DVD, memory cards, and external hard drives) used by staff and students. While the district recognizes the advantages for staff and students to maintain information on these devices, users are strongly encouraged to rely on their district provided storage 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.
- 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.

Non-District Managed Devices and Personally Owned Devices

The term "Non-District Managed Devices" is used to define any computing device (including personal laptops, desktops, tablets, and smartphones) used by staff and contractors. Users are strongly

encouraged to rely on their district provided device for all computing needs. When a staff member connects a district provided account to a non-district managed or personally owned device, they will be required to secure their device with a password or PIN. When using devices not managed by the district, staff and contractors should never transfer any documents labeled classified, confidential, or restricted to any non-district managed device or personal device.

Credit Card and Electronic Payment

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

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

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).

DRAFT

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, printers, 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. 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 (does not have salable value), it shall be handled according to one of the following methods. It is the responsibility of the technology department to update the inventory system to reflect the disposal of the asset.

Discard

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

DRAFT

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

Donation/Gift

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

DRAFT

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

Virus, Malware, and Spyware Protection

Oyster River Cooperative 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 Oyster River Cooperative 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 Microsoft 365 services.

Security Patches

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

DRAFT

Appendix J - Account Management

Access controls are essential for data security and integrity. The Oyster River Cooperative 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 Oyster River Cooperative 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 member is sent from Human Resources to the Technology Department. This notification includes position, building assignment(s), and start date.
- Only after notification has been received from Human Resources, the Technology Department creates user accounts. The user is given access and permissions to the necessary resources based on their position and building assignment(s) (see Appendix K: Data Access Roles and Permissions).
- Any exception to permissions must be approved by the district administrator responsible for the system (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.

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 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 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.

DRAFT

Appendix K - Data Access Roles and Permissions

Student Information System (SIS)

Staff are entered into the Oyster River Cooperative 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
- All School Administrator
- All Schools Attendance Only
- All Schools Nurse
- All Schools Read Only
- All Schools Registrar
- All Schools SPED Admin
- All Schools Teachers
- District Food Service
- Elementary Counselor
- IT Services
- HS AD & SRO
- HS Assistant Principal
- HS Attendance/Discipline
- HS Counseling
- HS Psychologist
- HS SPED Coordinator

DRAFT

- MS Counselor
- MS Demographics Only-No Grades
- MS PowerTeacher
- 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

- Employee Portal User
- Employee Portal Manager (Approver)
- Employee Portal SuperUser (Administrator)
- Finance System Requester
- Finance System Approver
- Finance System Directors
- Finance System Principals
- Finance System Super User (Administrator)

* 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
- IEP Team Member
- District Administrator
- SAU System Administrator
- SAU System Staff

- General Ed Teacher

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

Security Roles

- Web Roles
- Administrators
- UNH Intern
- Manager
- Vending Manager

Register Roles

- Cashier
- Manager
- Vendor Manager
- Time Clock Only
- Administrator

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

DRAFT

Appendix L - Password Security

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

- Passwords shall never be shared with another person.
- When possible, user created passwords should adhere to the same criteria as required for district network access as outlined below.
- Passwords shall never be saved when prompted by any application 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.

District network access to resources managed through LDAP/SSO:

- Passwords must be "strong," and must be a minimum of 10 characters long.
- Your password must not be too like your username.
- Do not use your district password for any non-district systems.
- Passwords will be changed annually.

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 repeated wrong passwords are entered in a short period of time.

DRAFT

Appendix M - Technology Disaster Recovery Plan

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to enable the Oyster River Cooperative School District (Oyster River Cooperative) 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 Oyster River Cooperative'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.
- District data is housed at district data center and backed up in the cloud.
- District data is hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, District networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

The Oyster River Cooperative has appointed the following people to the disaster recovery/critical failure team: Director of Technology, System Administrator, Network Administrator, and Information Systems Support 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. 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 will be notified as deemed appropriate in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- School Board
- District Staff
- Parents and Students
- Vendors including Insurance Company

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 Microsoft 365.

DRAFT

- Maintained secure application to store all system administrator accounts, passwords and vendor contact information. This will be accessible only to applicable Technology Staff who need access to perform their job functions.
- The District's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter and the cloud. The District's critical virtual servers can be run directly from the cloud with limited access.
- 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 Oyster River Cooperative's TDRP response will be conducted. This will entail gathering documentation from the response and feedback from all stakeholders and incorporate into an after action report and corrective action plan. The result will be an update to the TDRP and other emergency response plans as appropriate.

DRAFT

Appendix N - Data Breach Response Plan

Objectives

The purpose of the Technology Data Breach Plan (TDBP) is to enable the Oyster River Cooperative School District (Oyster River Cooperative) 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 Oyster River Cooperative's TDBP:

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

Data Breach/Incident Response Team

Oyster River Cooperative has appointed the following people to the data breach/incident response team: Superintend, Business Administrator, Director of Technology, System Administrator, Network Administrator, and Information Systems Support 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 be notified as deemed appropriate in the event the plan has been activated:

- Superintendent
- Superintendent's Leadership Team
- Technology Staff
- School Board
- District Staff
- Parents and Students
- Vendors including Insurance Company

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

DRAFT

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, System Administrator, Network Administrator, and Information Systems Support Specialists. Additional members of the Oyster River Cooperative 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 Oyster River Cooperative'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.

DRAFT

Policies for
First/Second Read/Adoption/Deletion
SB Meeting of
June 19, 2019

Title	Code
Policies for First Read	
Library & Instructional Materials Selections & Reconsideration	IJL
Facilities Use	KF
Policies for Second Read/Adoption	
Policies for Deletion/Replacement	

As a reference the June 12, 2019 policy minutes are attached to this packet.

Library and Instructional Materials Selection and Reconsideration Policy

Part 1: Selection of Instructional Materials and Library Resources

I. Objectives

The Oyster River Cooperative School Board recognizes its responsibility for all matters related to the District schools. The responsibility for the selection and coordination of instructional matters and other resources are delegated to the professional trained personnel employed by the school District in this capacity.

Instructional materials are selected by the school district to implement, enrich, and support the educational program. Materials will serve both the breadth of the curriculum and the needs and interests of the faculty and students. The district is obligated to provide a wide range of materials on all levels of difficulty and in a variety of formats, with diversity of appeal, and representing the presentation of many different points of view.

The objective of the Library is to make available to students and faculty a collection of materials that will enrich and support the curriculum and meet the needs and interests of the students and faculty served.

II. Responsibility for Selection

While the selection of materials involves many people including administrators, teachers, students, and community residents, the responsibility for coordinating and recommending the selection and purchase of library media materials rests with the Librarian. The responsibility for selecting instructional materials rests with the professional staff.

III. Criteria for Selection

The following general selection criteria will be used for the selection of library and instructional materials, including electronic, print, and non-print resources, as they apply:

1. Instructional materials and library resources shall support and be consistent with the general educational goals of the state and the district, and the aims and objectives of ORCSD and specific courses.

2. Instructional materials and library resources shall be chosen to enrich and support the curriculum and the personal needs and interests of users.

3. Instructional materials and library resources shall meet high standards of quality in:

    - Enrichment and support of the curriculum department
    - Accurate and unbiased depiction of the diversity and pluralistic nature of society
    - Matching the appropriate skill levels of students
    - Contribution to the curriculum and the educational goals of the school
    - Relevance to the interests of students and faculty
    - Reviews found in standard selection sources
    - Recommendations based on a preview examination of materials by professional personnel, adults with special expertise, or students

- Reputation and significance of the author, producer, and publisher
- Currency or timeliness of material
- Contribution to a breadth and diversity of representative viewpoints on controversial issues
- Contribution to multicultural and pluralistic awareness
- High degree of potential user appeal
- Quality, durability, and variety of format
- Suitability of format and appearance for intended use
- Value commensurate with cost and/or need

4. Instructional materials and library resources shall be appropriate for the subject area and for the age, emotional development, ability level, learning style, and social development of the students for whom the materials are selected.

5. Instructional materials and library resources shall be designed to provide a background of information that will motivate students and staff to examine their own attitudes and behavior; to comprehend their duties, responsibilities, rights and privileges as participating citizens in our society; and to make informed judgments in their daily lives.

6. Instructional materials and library resources shall provide information on opposing sides of controversial issues so that users may develop under guidance the practice of critical analysis.

IV. Selection of Learning Sources

In selecting materials for use, staff members will evaluate the materials and may consult reputable balanced critical assessments, review journals, specialists and/or professionally trained personnel employed by the School District. With the materials used in group instruction, school staff will pay particular attention to the experience and needs of their students in preparatory and follow-up activities.

- In selecting instructional materials and library resources, the Librarian or other professional staff members will evaluate available resources and curriculum needs and will consult reputable, professionally recognized reviewing periodicals, standard catalogs, and other selection aids to help guide the selection.

- Recommendations for purchase may involve administrators, teachers, students, parents, and community members, as appropriate.

- Gift materials shall be judged by the criteria outlined in this policy and shall be accepted or rejected by those criteria.

- Selection is an ongoing process that should include the removal of materials no longer appropriate and the replacement of lost and worn materials still of educational value.

V. Position on Intellectual Freedom

This school subscribes in principle to the statements of policy on library philosophy as expressed in the American Library Association' s *Library Bill of Rights,* a copy of which is appended to, and made a

questioned, the principles of intellectual freedom shall be defended.

Part 2: Procedures for Dealing with Challenged Materials

I. Statement of Policy

Despite the quality of the selection process, any parent/legal guardian or student may formally challenge instructional materials and library resources used in the school's educational program on the basis of appropriateness. The procedure concerning challenged materials is outlined below. Its purpose is to provide for a hearing with appropriate action, within the context of the principles of freedom of information, the student's right to access information, and the professional responsibility and integrity of the school faculty. No materials shall be removed from ORCSD before the process of review is completed.

II. Preliminary Complaint Request

Upon receiving a complaint:

1. The librarian [or Principal, or other appropriate staff member] shall explain to the questioner the school's selection procedure, criteria, and qualifications of those persons selecting the resource.

2. The librarian [or other appropriate staff member] shall explain the particular place the questioned resource occupies in the educational program, its intended usefulness, and additional information regarding its use, or refer the party to someone who can identify and explain the use of the resource.

3. If the questioner wishes to file a formal challenge, a copy of the *ORCSD School Library and Instructional Materials Selection and Reconsideration Policy* and a *Request for the Reconsideration of Instructional Materials and Library Resources* form [Appendix C] shall be emailed to the party concerned by the library media director, along with a letter to the complainant [Appendix D].

III. Request for Formal Reconsideration

A) Preliminary Procedures

1. The questioner must read or review the material in question in its entirety.

2. ORCSD will keep on hand and make available the *Request for Reconsideration of Instructional Materials and Library Resources* forms [Appendix C]. All formal objections to instructional materials and library resources must be made on these forms.

3. The Request for Reconsideration of Instructional Materials and Library Resources form shall be completed and signed by the questioner before further consideration will be given. The form shall be filed with the principal. If the form is not completed and returned, it shall be assumed that the questioner no longer wishes to file a formal complaint [as stated in the letter to complainant, [Appendix D.]

4. The superintendent shall be informed of the formal complaint received.

5. The request for reconsideration shall be referred to a reconsideration committee at the school level for reevaluation of the resource.

B) The Reconsideration Committee

1. Upon receipt of a request for the reconsideration of Instructional Materials and Library Resources, [Appendix C] the reconsideration committee shall arrange to meet within twenty working days after the complaint is received.

The Librarian will select and chair, with the support from the building principal, a reconsideration committee selected for diversity of opinion and relevant expertise.

The reconsideration committee will consist of:

- Members of the teaching staff,
- A school administrator, appointed by the administrative team
- Up to two students, as age appropriate
- ~~Up to~~ two adults, appointed by the Superintendent

2. The reconsideration committee shall review the challenged resource and judge whether it conforms to the principles of selection outlined in the *ORCSD School Library and Instructional Materials Selection and Reconsideration Policy.*

3. The identity of committee members will remain anonymous.

C) Resolution

1. The reconsideration committee shall:

   a. Examine the challenged resource in its entirety
   b. Determine professional acceptance by reading critical reviews of the resource
   c. Weigh values and faults, and form opinions based on the material as a whole rather than on passages or selections taken out of context
   d. Discuss the challenged resource in the context of the educational program
   e. Discuss the challenged item with the individual questioner when appropriate
   f. Prepare a written report

2. The written report shall be discussed with the individual questioner if requested.

3. The librarian shall retain the written report with copies forwarded to the superintendent, and the principal.

4. Notwithstanding any procedure outlined in this policy, the questioner shall have the right to appeal any decision of the reconsideration committee to the Superintendent whose sole role is to review the process used for consistency but will not supersede the integrity and thoroughness of the final recommendations of the review committee.

D) Guiding Principles

1. Parent/Legal Guardian or student may raise objection to instructional materials and library resources used in ORCSD educational program, despite the fact that the individuals selecting such resources were duly qualified to make the selection, followed the proper procedure, and observed the criteria for selecting instructional materials and library resources.

2. The librarian should review the selection and objection rules with the teaching staff at least annually. The staff should be reminded that the right to object to instructional materials and library resources is one granted by policies enacted by the school board.

3. No parent has the right to determine reading, viewing, or listening matter for students other than his or her own children.

4. ORCSD supports the *Library Bill of Rights* and *The Freedom to Read Statement,* adopted by the American Library Association [Appendixes A and BJ. When instructional materials and library resources are challenged, the principles of the freedom to read/listen/view must be defended as well.

5. Access to challenged material shall not be restricted during the consideration process.

6. A decision to sustain a challenge shall not necessarily be interpreted as a judgment of irresponsibility by the professionals involved in the original selection and/or use of the material.

List of Appendix's

Appendix A – Library Bill of Rights
Appendix B – The Freedom to Read Statement
Appendix C – Request for the Reconsideration of Instructional Materials and Library Resources
Appendix D – Sample Letter to Complainant

Appendix A

Library Bill of Rights

The American Library Association affirms that all libraries are forums for information and ideas, and that the following basic policies should guide their services.

I. Books and other library resources should be provided for the interest, information, and enlightenment of all people of the community the library serves. Materials should not be excluded because of the origin, background, or views of those contributing to their creation.

II. Libraries should provide materials and information presenting all points of view on current and historical issues. Materials should not be proscribed or removed because of partisan or doctrinal disapproval.

III. Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment.

IV. Libraries should cooperate with all persons and groups concerned with resisting abridgment of free expression and free access to ideas.

V. A person's right to use a library should not be denied or abridged because of origin, age, background, or views.

VI. Libraries which make exhibit spaces and meeting rooms available to the public they serve should make such facilities available on an equitable basis, regardless of the beliefs or affiliations of individuals or groups requesting their use.

VII. All people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information.

© American Library Association Adopted June 19, 1939, by the ALA Council; amended October 14, 1944; June 18, 1948; February 2, 1961; June 27, 1967; January 23, 1980; January 29, 2019.

Inclusion of "age" reaffirmed January 23, 1996.

Appendix B

The Freedom to Read Statement

The freedom to read is essential to our democracy. It is continuously under attack. Private groups and public authorities in various parts of the country are working to remove or limit access to reading materials, to censor content in schools, to label "controversial" views, to distribute lists of "objectionable" books or authors, and to purge libraries. These actions apparently rise from a view that our national tradition of free expression is no longer valid; that censorship and suppression are needed to counter threats to safety or national security, as well as to avoid the subversion of politics and the corruption of morals. We, as individuals devoted to reading and as librarians and publishers responsible for disseminating ideas, wish to assert the public interest in the preservation of the freedom to read.

Most attempts at suppression rest on a denial of the fundamental premise of democracy: that the ordinary individual, by exercising critical judgment, will select the good and reject the bad. We trust Americans to recognize propaganda and misinformation, and to make their own decisions about what they read and believe. We do not believe they are prepared to sacrifice their heritage of a free press in order to be "protected" against what others think may be bad for them. We believe they still favor free enterprise in ideas and expression.

These efforts at suppression are related to a larger pattern of pressures being brought against education, the press, art and images, films, broadcast media, and the Internet. The problem is not only one of actual censorship. The shadow of fear cast by these pressures leads, we suspect, to an even larger voluntary curtailment of expression by those who seek to avoid controversy or unwelcome scrutiny by government officials.

Such pressure toward conformity is perhaps natural to a time of accelerated change. And yet suppression is never more dangerous than in such a time of social tension. Freedom has given the United States the elasticity to endure strain. Freedom keeps open the path of novel and creative solutions and enables change to come by choice. Every silencing of a heresy, every enforcement of an orthodoxy, diminishes the toughness and resilience of our society and leaves it the less able to deal with controversy and difference.

Now as always in our history, reading is among our greatest freedoms. The freedom to read and write is almost the only means for making generally available ideas or manners of expression that can initially command only a small audience. The written word is the natural medium for the new idea and the untried voice from which come the original contributions to social growth. It is essential to the extended discussion that serious thought requires, and to the accumulation of knowledge and ideas into organized collections.

We believe that free communication is essential to the preservation of a free society and a creative culture. We believe that these pressures toward conformity present the danger of limiting the range and variety of inquiry and expression on which our democracy and our culture depend. We believe that every American community must jealously guard the freedom to publish and to circulate, in order to preserve its own freedom to read. We believe that publishers and librarians have a profound responsibility to give validity to that freedom to read by making it possible for the readers to choose freely from a variety of offerings.The freedom to read is guaranteed by the Constitution. Those with faith in free people will stand firm on these constitutional guarantees of essential rights and will exercise the responsibilities that accompany these rights.

We therefore affirm these propositions:

1. *It is in the public interest for publishers and librarians to make available the widest diversity of views and expressions, including those that are unorthodox, unpopular, or considered dangerous by the majority.*

   Creative thought is by definition new, and what is new is different. The bearer of every new thought is a rebel until that idea is refined and tested. Totalitarian systems attempt to maintain themselves in power by the ruthless suppression of any concept that challenges the established orthodoxy. The power of a democratic system to adapt to change is vastly strengthened by the freedom of its citizens to choose widely from among conflicting opinions offered freely to them. To stifle every nonconformist idea at birth would mark the end of the democratic process. Furthermore, only through the constant activity of weighing and selecting can the democratic mind attain the strength demanded by times like these. We need to know not only what we believe but why we believe it.

2. *Publishers, librarians, and booksellers do not need to endorse every idea or presentation they make available. It would conflict with the public interest for them to establish their own political, moral, or aesthetic views as a standard for determining what should be published or circulated.*

   Publishers and librarians serve the educational process by helping to make available knowledge and ideas required for the growth of the mind and the increase of learning. They do not foster education by imposing as mentors the patterns of their own thought. The people should have the freedom to read and consider a broader range of ideas than those that may be held by any single librarian or publisher or government or church. It is wrong that what one can read should be confined to what another thinks proper.

3. *It is contrary to the public interest for publishers or librarians to bar access to writings on the basis of the personal history or political affiliations of the author.*

   No art or literature can flourish if it is to be measured by the political views or private lives of its creators. No society of free people can flourish that draws up lists of writers to whom it will not listen, whatever they may have to say.

4. *There is no place in our society for efforts to coerce the taste of others, to confine adults to the reading matter deemed suitable for adolescents, or to inhibit the efforts of writers to achieve artistic expression.*

   To some, much of modern expression is shocking. But is not much of life itself shocking? We cut off literature at the source if we prevent writers from dealing with the stuff of life. Parents and teachers have a responsibility to prepare the young to meet the diversity of experiences in life to which they will be exposed, as they have a responsibility to help them learn to think critically for themselves. These are affirmative responsibilities, not to be discharged simply by preventing them from reading works for which they are not yet prepared. In these matters' values differ, and values cannot be legislated; nor can machinery be devised that will suit the demands of one group without limiting the freedom of others.

5. *It is not in the public interest to force a reader to accept the prejudgment of a label characterizing any expression or its author as subversive or dangerous.*

The ideal of labeling presupposes the existence of individuals or groups with wisdom to determine by authority what is good or bad for others. It presupposes that individuals must be directed in making up their minds about the ideas they examine. But Americans do not need others to do their thinking for them.

6. *It is the responsibility of publishers and librarians, as guardians of the people's freedom to read, to contest encroachments upon that freedom by individuals or groups seeking to impose their own standards or tastes upon the community at large; and by the government whenever it seeks to reduce or deny public access to public information.*

   It is inevitable in the give and take of the democratic process that the political, the moral, or the aesthetic concepts of an individual or group will occasionally collide with those of another individual or group. In a free society individuals are free to determine for themselves what they wish to read, and each group is free to determine what it will recommend to its freely associated members. But no group has the right to take the law into its own hands, and to impose its own concept of politics or morality upon other members of a democratic society. Freedom is no freedom if it is accorded only to the accepted and the inoffensive. Further, democratic societies are more safe, free, and creative when the free flow of public information is not restricted by governmental prerogative or self-censorship.

7. *It is the responsibility of publishers and librarians to give full meaning to the freedom to read by providing books that enrich the quality and diversity of thought and expression. By the exercise of this affirmative responsibility, they can demonstrate that the answer to a "bad" book is a good one, the answer to a "bad" idea is a good one.*

   The freedom to read is of little consequence when the reader cannot obtain matter fit for that reader's purpose. What is needed is not only the absence of restraint, but the positive provision of opportunity for the people to read the best that has been thought and said. Books are the major channel by which the intellectual inheritance is handed down, and the principal means of its testing and growth. The defense of the freedom to read requires of all publishers and librarians the utmost of their faculties and deserves of all Americans the fullest of their support.

We state these propositions neither lightly nor as easy generalizations. We here stake out a lofty claim for the value of the written word. We do so because we believe that it is possessed of enormous variety and usefulness, worthy of cherishing and keeping free. We realize that the application of these propositions may mean the dissemination of ideas and manners of expression that are repugnant to many persons. We do not state these propositions in the comfortable belief that what people read is unimportant. We believe rather that what people read is deeply important; that ideas can be dangerous; but that the suppression of ideas is fatal to a democratic society. Freedom itself is a dangerous way of life, but it is ours.

This statement was originally issued in May of 1953 by the Westchester Conference of the American Library Association and the American Book Publishers Council, which in 1970 consolidated with the American Educational Publishers Institute to become the Association of American Publishers. Adopted June 25, 1953, by the ALA Council and the AAP Freedom to Read Committee; amended January 28, 1972; January 16, 1991; July 12, 2000; June 30, 2004.

Appendix C

Request for the Reconsideration of Instructional Materials and Library Resources

Request Initiated by: _____

Telephone: _____ Address: _____

Town: _____

Complainant is ☐ student ☐ parent/guardian of student

Complainant represents: _____himself/herself

_____name of group

_____other: _____

Resource on which you are commenting:

_____Book _____Video _____Other

_____Magazine _____CD

_____Newspaper _____Website

Author/Producer: _____

Title: _____

Publisher: _____

Please answer the following questions either in the space provided, or on additional pages.

1. Have you been able to discuss this work with the teacher or librarian who ordered it or who used it?

_____Yes _____No

2. Did you read the entire book, or view the entire material? If not, which parts?

3. What do you think is the theme of this book or material?

4. To what in the book/material do you object? Be specific. Cite pages, or passages.

5. Is there anything good about this book/material?

6. What do you feel might be the result of reading this book, or using this material?

7. For what age group would you recommend this book/material?

8. Describe what you understand to be the judgement of this book, or material, by critics.

9. In its place, what work would you recommend that would convey as valuable a picture and perspective of the subject treated?

_____ _____

Date Signature of Complainant

This form is based on materials developed by the National Coalition of English Teachers and is used with permission. Revisions are authorized and sponsored by the ORCSD School Board, and not the NCTE.

Appendix D

Sample Letter to Complainant

Date

Dear:

We appreciate your concern over the use of _____ at

the Oyster River Cooperative School: _____.

The school has developed procedures for selecting materials but realizes that not everyone will agree with every selection made.

To help you understand the selection process, we are sending a copy of Oyster River's *Library and Instructional Materials Selection and Reconsideration Policy*.

If you are still concerned after you review this material, please complete the *Request for the Reconsideration of Learning Resources form* and return it to me. You may be assured of prompt attention to your request. If I have not heard from you within two weeks from the date listed above, we will assume you no longer wish to file a formal complaint.

Sincerely,

Librarian

OYSTER RIVER COOPERATIVE SCHOOL BOARD	Policy Code: KF Previously: KG
School Board First/Second Read: November 7, 2012/November 14, 2012 Policy Review: February 4, 2014 School Board First/Second Read: March 5, 2014/April 2, 2014 Policy Committee Review: August 8, 2018 School Board First/Second/Adoption: August 15, 2018 Policy Committee Review: May 8, 2019 & June 12, 2019 School Board First Read: June 19, 2019	Page 1of 3 Category: Recommended

USE OF SCHOOL BUILDINGS AND FACILITIES

The Oyster River School Board ~~accepts the responsibility for making~~ allows its facilities to be used by ~~available to~~ responsible organizations, associations, and individuals of the community for appropriate civic, cultural, welfare or recreational activities which do not interfere with school activities ~~infringe upon nor interfere with the conduct~~ and is in the best interests of the school system. Authorization to use school facilities does not connote Board endorsement or approval of the activity or of the sponsoring organization/individual.

Policies

The Organization shall ensure that staff, students, and all participants in the PROGRAM shall follow all policies and rules of the Oyster River Cooperative School District to ensure the safety of all participants and the care of the facilities.

The Organization shall further ensure that the PROGRAM is operated in a manner that conforms to the School Board's Policy AC (Nondiscrimination/Equal Opportunity) and permits the School District to meet its obligations under federal and state non-discrimination laws.

The School District Rules can be found in the Parent Student Handbook on the District website under the school tab for each school, and the School Board Policies at:
http://www.orcsd.org/schoolboard/policies

Prohibited:

Any activity or organization which:

1. Promulgates any theory or doctrine subversive to the laws of the United States, the State of New Hampshire or any political subdivision thereof.
2. Advocates governmental change by violence.
3. Violates the canons of good morals, manners or taste, or is injurious to the district buildings, grounds or equipment.
4. Is in conflict with school activities or programs or policies.
5. Raises funds for any purpose except as permitted by board policy or special action of the board.
6. Is discriminatory.

Granting of Approval:

The Superintendent of schools or designee is authorized to approve and arrange for scheduling the use of school facilities by applicants satisfying the above requirements.

~~Right is reserved by~~ Tthe ~~board~~ Board authorizes the Superintendent to revoke any such permit, without liability, should such action be deemed necessary or desirable.

Applicants may be required to submit an explanatory statement declaring that to the best of their knowledge the projected use is within the general policy and is not in violation of prohibited activities noted above.

Fees:

The Board will approve a schedule of fees for use of school facilities. The Superintendent or designee(s) may grant waivers of fee payment in exceptional cases. The Board intends that recognized parent volunteer groups, such as PTO's, will not be charged fees for use of facilities that have approval of the building Principal and Business Administrator. Fee schedule will be reviewed as part of the annual

budget process.

OYSTER RIVER COOPERATIVE SCHOOL BOARD	Policy Code: KF Previously: KG
School Board First/Second Read: November 7, 2012/November 14, 2012 Policy Review: February 4, 2014 School Board First/Second Read: March 5, 2014/April 2, 2014 Policy Committee Review: August 8, 2018 School Board First/Second/Adoption: August 15, 2018 Policy Committee Review: May 8, 2019 & June 12, 2014 School Board First Read: June 19, 2019	Page 2 of 3

USE OF SCHOOL BUILDINGS AND FACILITIES (continued)

~~Certificates of~~ Insurance:

Each application for school rental will include a certificate of insurance for general liability and property damage, the coverage to be as recommended by the district's insurance carrier. The Superintendent or designee(s) may grant waivers of certificate of insurance in exceptional cases, and shall not cause such policy to be terminated or materially changed without giving the Board at least 10 days' prior written notice. The Organization shall maintain workers compensation insurance as required by state law. The organization shall provide the Board with proof of insurance upon request. The Oyster River Cooperative School District shall be listed on the certificate ~~as~~ and named as an additional ~~named~~ insured.

Damages:

Anyone submitting an application for the rental of school property must assume responsibility for the proper use of the facility and for the conduct of all attending the event. As a condition for permission to use the facility the user must indemnify the school district from any claims which might arise from the use. If any school district property is lost or damaged during usage, the amount of loss or damage will be determined by the superintendent of schools, and a bill for damages (both labor and materials) will be mailed to the applicant of record, who accepts responsibility for payment of damages as a condition for permission to use the facility. In addition, the Superintendent or designee may require the submission of a deposit in advance to cover any potential loss or damage to school district property.

Complaints:

1. If an incident occurs that could be viewed as a violation of district policy or procedure, the district will be informed. ORCSD reserves the right to examine the incident and determine if it impacts further facilities use.
2. Every effort will be made to resolve the issue at the lowest level.
3. Complaints that result in investigations of violation of district policies will be conducted by independent third parties at the expense of the group using ORCSD Facilities.

Indemnification:

The organization agrees to defend, indemnify and hold harmless ORCSD for any claims, liability, or damages, arising out of the Organization's use of space under this Agreement.

~~Insurance:~~

~~During the term of this Agreement the Organization shall maintain in effect a policy of general public liability insurance with limits of at least $1,000,000 for bodily injury (per occurrence) and $1,000,000 for property damage (per occurrence) the Organization shall cause the Oyster River School to be named as additionally insured on such insurance policy and shall not cause such policy to be terminated or materially changed without giving the Board at least 10 days' prior written notice. The Organization shall maintain workers compensation insurance as required by state law. The Organization shall provide the Board with proof of insurance upon request.~~

Receipts:

Receipts from fees shall be used for facilities maintenance and operation costs.

OYSTER RIVER COOPERATIVE SCHOOL BOARD	Policy Code: KF Previously: KG
School Board First/Second Read: November 7, 2012/November 14, 2012 Policy Review: February 4, 2014 School Board First/Second Read: March 5, 2014/April 2, 2014 Policy Committee Review: August 8, 2018 School Board First/Second/Adoption: August 15, 2018 Policy Committee Review: May 8, 2019 & June 12, 2019 School Board First Read: June 19, 2019	Page 3 of 3

Regulations:

Regulations governing this policy shall be posted on the school district web site.

Cross Reference:

AC- Nondiscrimination/Equal Opportunity
ACE & R – Nondiscrimination on Basis of Handicap/Disability & Procedure
GBA – Equal Opportunity Employment
GBAA & R & 1 – Sexual Harassment – Employee/Staff & Procedure & Report Form
JBAA & R– Sexual Harassment and Violence -Students & Procedure
JBAB & R – Transgender and Gender Nonconforming & Procedure
KF-R Guidelines on the Use of School Facilities
KF-R1 Building Rental Fees
JLCF – Wellness Policy
JL – Soliciting Funds
KFB – Advertising in Schools

Legal Reference: Military Recruitment in high schools