School District of Manawa

Policy & Human Resources COMMITTEE MEETING

Manawa School District Office - Board Room
800 Beech Street, Manawa WI
(920)596-2525

Monday, July 17, 2023
6:15 P.M.

Board of Education Committee Members:
Reierson (C), Hansen, & Krueger

- **CALL TO ORDER**
- **PLEDGE OF ALLEGIANCE**
- **ROLL CALL** - *Verification of Quorum*
  - *B.O.E. Members Present:*
- **COMPLIANCE WITH OPEN MEETING LAW NOTIFICATION** *[§19.84(2) Wis. Stats.]*
- **AGENDA**

1. Discuss the addition of a Nutrition Program Director position. (Information/Action)
2. Discuss Hourly employee timekeeping process - there are concerns that hourly employee actual work time is not being captured consistently so that we are paying them accurately. (Information/Action)
3. Discuss CESA 6 school site days - support we are contracting with CESA 6 on, if they are on-site, how often, etc. (Information/Action)
4. Discuss and propose a method to address Salary Advancement Points for Professional Educators who are part of the adjustment process. (Information/Action)
5. Consider Endorsement of Merging the Laude and Weighted Grade System. (Information/Action)
    a. Review Policies for any needed revisions.
6. Consider Endorsement of the presented NEOLA policy deletions from the combined Staff policy changes (see 06/21/23 committee meeting packet). (Information/Action)
7. Consider Endorsement of the following Handbooks/Procedures for the 2023-24 school year (list of Handbooks can be found in the Special Board meeting file of 06/20/23): (Information/Action)
    a. SDM Chromebook Program

* Any person with a qualifying disability under the Americans with Disabilities Act that requires the meeting or material to be in accessible format, please contact the District Administrator to request reasonable accommodation. The meeting room is wheelchair accessible. This meeting is a meeting of the Board of Education in public for the purpose of conducting the School District's business and is not to be considered a public hearing. There may be a time for public comment during the meeting as indicated in the agenda.

**Upon request to the District Administrator, submitted twenty-four (24) hours in advance, the District shall make reasonable accommodations including the provision of informational material in an alternative format for a disabled person to be able to attend this meeting.

School District of Manawa

Policy & Human Resources COMMITTEE MEETING

Manawa School District Office - Board Room
800 Beech Street, Manawa WI
(920)596-2525

   b. Information Technology Plan
   c. Coaches Handbook
   d. Cyber Incident Response and After Action
8. Consider adding a Transgender policy. (Information/Action)
9. Consider adding Policy regarding Artificial Intelligence. (Information/Action)
10. Discuss compliance of Website based on July 2022 P&HR committee meeting notation *->> Special note regarding Handbook Annual Review: Handbooks will be posted to the School District of Manawa website following Board of Education approval of substantive language changes as presented. The Manawa Board of Education will be notified of the date that this handbook (or plan as appropriate) is converted to a version considered compatible for use by individuals with visual impairments or limited vision as per the Office of Civil Rights requirements and posted to the School District of Manawa website. This OCR compatible conversion may impact the appearance of the document (i.e. change in fonts, font sizes, paging in the table of contents, etc.) resulting in technical changes but no substantive changes will be made. Should a substantive change be required, the handbook (plan) will be brought back to the Board of Education for approval.* **Has our legal responsibility been approved?** (Information/Action)
11. Discuss creating a Daycare area within the District buildings. (Information/Action)
12. Discuss Orientation and On-Boarding Process. (Information/Action)
13. Discuss defining Subject Matter Experts (SME's) to write Standard Operating Procedures (SOP's). Development of SOP's is important for supporting existing job duties and for supporting new employees who may be coming into new job duties. (Information/Action)
14. Discuss and propose an update to the mileage and reimbursement process. (Information/Action)
15. Discuss Policy concerning electronics being used for District business and the ability of employees to purchase District owned electronics. (Information/Action)

- **FUTURE MEETING AGENDA ITEMS & MEETING DATES/TIMES**
  - ➢

- **ADJOURN**

* Any person with a qualifying disability under the Americans with Disabilities Act that requires the meeting or material to be in accessible format, please contact the District Administrator to request reasonable accommodation. The meeting room is wheelchair accessible. This meeting is a meeting of the Board of Education in public for the purpose of conducting the School District's business and is not to be considered a public hearing. There may be a time for public comment during the meeting as indicated in the agenda.

**Upon request to the District Administrator, submitted twenty-four (24) hours in advance, the District shall make reasonable accommodations including the provision of informational material in an alternative format for a disabled person to be able to attend this meeting.

SDM Chromebook Program Handbook

Approved by the School District of Manawa
Board of Education 07-17-2023

SDM Chromebook Program

Program Handbook

Table of Contents

SDM Chromebook Program

Program Handbook

Overview

Technology is a key component of the modern school environment. The School District of Manawa provides each student with a Chromebook device for school use. The details below describe the existing 1:1 environment as well as proposed changes for the future of the program.

Note: This handbook includes several links to other resources. It is recommended that this document is read electronically instead of printed.

Program Goals

Use technology to create a platform for students to learn. This program provides tools to be more efficient and learn in new ways. The table below describes how the Chromebook program contributes to meeting the ISTE Standards for Students.

SDM Chromebook Program and ISTE Standards	
Empowered Learner	Improved tools to expand learning goals and reflect on their learning process. Greater access to internet allows students to build networks and learn in ways they could not otherwise.
Digital Citizen	Student learn to manage their personal identity in a digital world. Students are expected to act in safe, legal, and respectful ways.
Knowledge Constructor	Students have a tool more efficiently research information and build knowledge.
Innovative Designer	Greater access to online tools to learn in authentic cyclical design processes.
Computational Thinking	Student have a tool to take part in analytical problem solving.
Creative Communicator	Students have opportunities to express themselves through digital media such as blogs and videos.
Global Collaborator	Students can better connect with other cultures and experts globally.

Software

Productivity Software

Google G Suite

Manawa is a Google school district. Students and staff use the Google G Suite for document, worksheet, and presentation software.

Google Classroom

We use Google Classroom as our learning management system (LMS). A LMS allows teachers to create an online space for organizing their classroom. Assignments, formative assessments, and other resources are typically shared with students through an LMS.

Creativity Software

Loom

This tool allows students to record videos using their Chromebooks. The videos may include their web camera or desktop. This allows them to demonstrate knowledge using media as well as written word.

Flipgrid

This is another valuable tool available to our education community. Flipgrid allows teachers to prompt students to create short video responses to questions.

Classroom Management & Web Filter

GoGuardian

We are working to help teachers better use GoGuardian to manage student use of devices. Our strategy is to provide short professional development sessions throughout the school year and offer 1-on-1 help as needed. GoGuardian has been a successful component of our Chromebook program. Going forward we need to continue supporting teacher use and encourage them to explore more advanced features.

Professional Development

Technology is only effective if teachers are effective using technology. Professional development is key to help teachers master the tools available. Teachers are encouraged to ask for help from IT or Library staff on a one-on-one basis. Professional development needs to be part of our culture instead of an occasional event. During the summer of 2020 we hosted twenty-five online and in-person training sessions to prepare for the fall.

Device Rotation

Chromebook have a reliable duty cycle of 5-7 years. No device should be assigned to a student that is older than five years. The Acer laptops purchased in 2014 and 2015 will be used for five years to allow us to establish a sustainable cycle.

Chromebook Repair

A smooth repair process is key to the success of the Chromebook 1:1 program. This document outlines how students can have their device serviced. We also outline the responsibilities of library, teachers, and technology.

Chromebook Repair Process

Student Responsibility

Students are expected to use technology in a way that is safe, legal, and respectful of others. Every year secondary students and parents sign our Technology Acceptable Use and Safety Form. Students who fail to meet these standards may have their access to the internet restricted.

Technology Acceptable Use and Safety Form
Restricted Student Access

Student Security, Privacy, and Safety

Encouraging students to explore the internet comes with increased risk. To address this concern

Students as Digital Citizens

Students must learn to become digital citizens that protect their online identities. They need to understand how to recognize and avoid risks while using technology.

Web Filters

The SDM uses technology to limit risk to students. These include GoGuardian for Chromebook devices and an iBoss web filter while at school.

Software Security, Privacy, and Safety Rubric

The SDM must protect student Personally Identifiable Information (PII). Any software system which requires students to create an account or otherwise uses PII data must be compared to our SSPS rubric. Any software system which fails to meet these standards may not be used by students.

Software Security, Privacy, & Safety Rubric

SDM Chromebook Program

Program Handbook

Budget

The proposed Chromebook rotation cycle requires 50 to 60 new chromebooks annually. This allows the following grade levels to receive new devices. Devices have already been purchased for the 2021-22 school year.

- Grade K
- Grade 5
- Grade 10

Item	Unit Cost	Count	Extended
Chromebook	$280.00	50	$14000
Chrome Management License	$33.00	50	$1650
Replacement Parts			$3,000
		Estimate Annual Cost	$18650

Chromebook Extensions

Starting with the 2018-19 school year students are only allowed to use pre-approved chromebook extensions on school Chromebook devices. The change was made primarily for security reasons to prevent the use of VPN and malware software from reaching our network. Another important reason is to reduce distractions in the classroom.

Staff may request additions to this list by contacting the technology director.

Allowed Extensions

Extension Name	**Offered By**	**Notes**
Google+	Google	
Office Editing for Docs, Sheets & Slides	Google	

EasyBib Toolbar	Easybib.Com	
Google Drive	Google	
Google Maps	Google	
Google Keep - notes and lists	Google	
Google Play Music	Google	
Google Photos	Google	
Google Forms	Google	
Gmail	Google	
Google Sheets	Google	
Home - New Tab Page	Google	
GeoGebra Classic	https://www.geogebra.org	
Google Play Books	Google	
Calculator	Chrome OS	
Evernote Web	EverNote.Com	
Evernote Web Clipper	EverNote.Com	
Grammarly for Chrome	grammarly.com	
e-clock	Yuriy Husnay	
Text	text.app	
Google Docs Offline	Google	
Google Calendar	Manas Tungare	
Google Cast for Education	developers.google.com/cast	
YouTube	www.youtube.com	
Google Cast	Google	

Google Drawings	Google	
Google Slides	Google	
Read&Write for Google Chrome		Purchased license for entire district.
Calculator	http://scientific-calculator.appspot.com/	
Camera	chromeos-cameraapp	
Spotify	open.spotify.com	
Sticky Notes	ProWebJect	
Gmail Offline	https://mail.google.com/mail/mu	
Google Docs	Google	
Kami	kamihq.com	
Vernier Graphical Analysis	www.vernier.com	
Cite This For Me (Free) Cite This For Me	www.citethisforme.com	

Force Installed Extensions

Several extensions are automatically installed on all student Chromebooks. These extensions are described below. Staff may request an extensions to be automatically installed by contacting the technology director.

Extension Name	**Offered By**	**Notes**
Office Editing for Docs, Sheets & Slides	Google	
Google Drive	Google	

Google Forms	Google	
Google Sheets	Google	
Google Drawings	Google	
Google Slides	Google	
Google Docs	Google	
Calculator	http://scientific-calculator.appspot.com/	
DRC Insight	DRCIS	This will be removed and re-installed twice a year.
iBoss SSO Integration		
Big Ideas Math	Big Ideas Learning, LLC	
uBlock Origin	Raymond Hill (gorhill)	Ad blocking software
Vernier Graphical Analysis		
Dyslexia Reading Assistant	CrayonMelon	
OpenDyslexic Font for Chrome	abbiecod.es	

Purchase History

This portion of the handbook describes the district purchase history since the beginning of the Chromebook program.

- 2014:
  - The initial order of Acer 720 Chromebooks were ordered. All students from grades 7-12 were supplied with a device.
- 2015:
  - An order of Acer 740 Chromebooks were ordered to supplement the initial order. It is difficult to know the exact number of devices that were ordered in 2015.
- 2016:
  - The district switched from Acer to Dell Chromebooks in the secondary school.
  - Some devices were ordered to supplement the Acer devices in the secondary school.
  - Acer R11 Touchscreen devices were supplied for each 6th grade classroom.
- 2017:
  - 70 Dell 11 Chromebooks were ordered for the secondary school. 9th Grade students were the primary recipients of these devices.
- 2018
  - 130 Dell 11 Chromebooks were ordered. 6th and 9th grade students received new devices. Acer R11 devices were reallocated to kindergarten, grade 1, and select special education classrooms.
  - Grade 4 and 5 chromebook carts provide one device per two students.
  - Grade 1, 2, and 3 chromebook cards provide one device per three students. Some of these classrooms have classroom sets of 4-5 devices.
- 2019
  - 140 Dell 11 Chromebooks were ordered.
  - Older devices were distributed to lower grades similar to 2018
- 2020 & 2021
  - The initial plan was to order 140 non-touch screen devices. Plus, an additional 50 touch screen devices. Due to the pandemic, we expanded the Chromebook program to include all students. The order was expanded to 370 Lenovo touch screen devices.
  - Due to delays associated with the COVID-19 and a microchip shortage, our order was delayed until February 2021.

    - To ensure no delays for the next school year, the district purchased the supply of Chromebooks for the 2021-22 school year early. An additional 270 Lenovo touch screen devices were ordered
    - No chromebooks are planned to be ordered during the summer of 2021.
- 2021 & 2022
    - Ordered 240 touch screen chromebooks through the ECF funding (special one time Covid funding)
- 2022 & 2023
    - Closed chromebook leasing contracts
    - Deployed new chromebooks removing the Acer/Lenovo units from classrooms on an as needed basis

School District of Manawa

Technology Plan

SDM Technology Plan Update

Submitted June 2022

Table of Contents

Successful Technology Plan

What is a Technology Plan

At its most basic level, a technology plan is a high-level strategy that details where your organization is now and where it wants to go in the future with respect to technology and infrastructure. Some plans concentrate on the acquisition of hardware or the development of network infrastructure. This plan includes how classroom technology is used to enhance learning.

These are important components of an effective plan. Barnet (2001) has clearly and succinctly defined 10 essential elements of a successful technology plan.

- Create a vision
- Involve all stakeholders
- Gather data
- Review the research
- Integrate technology into the curriculum
- Commit to professional development
- Ensure a sound infrastructure
- Allocate appropriate funding and budget
- Plan for ongoing assessment and monitoring
- Prepare for tomorrow

Why is a Technology Plan Important

Having a technology plan helps you prioritize and allocate your resources appropriately in order to achieve your goals on time and within budget. It provides transparency with respect to the goals and, by extension, creates greater buy-in from leadership and staff. (Stockert 2017)

Note: This handbook includes several links to other resources. It is recommended that this document is read electronically instead of printed.

Technology Needs Assessment

Technology Infrastructure Lifecycle

This included a long-term plan for replacement of essential infrastructure equipment. This plan should estimate the cost and suggest a potential source for funding.

- Storage devices
- UPS equipment
- Data backup and recovery
- Moving Data structures to the cloud

Expanded Disaster Recovery Plan

Plan for and implement improvements to our disaster recovery process to limit risk to malware attacks including phishing and ransomware.

Desktop Office and Presentation Station Lifecycle

Desktop computers in all offices and classrooms life cycle will be extended by the use of Solid State Drives.

Technology Goals

Task	Description	Target Date
Technology PD Planning	Continue to develop technology PD plan	End of SY 2023-24
Improve Disaster Recovery Plan	Improve DR plan to address ransomware and other TBD threats.	End of SY 2023-24
District-wide adoptoption of ISTE framework	Continue implementation of ISTE standards.	End of SY 2023-24

Teaching, Learning, and Technology Integration

TLTI is the plan to support the effective use of technology in the classroom. Technology should allow students to learn more efficiently or in ways not otherwise possible. TLTI is about supporting teachers as they integrate technology into instruction.

Chromebook 1-to-1 Program

Technology is a key component of the modern school environment. The School District of Manawa provides each student with a Chromebook device for school use. The following documents describe the SDM Chromebook program in greater depth.

- SDM Chromebook Program: Program Handbook (See Separate Handbook)
- Technology Acceptable Use and Safety Form (See Appendix A)
- Software Security, Privacy, and Safety Rubric (See Appendix B)

Professional Development

A successful professional development program prepares teachers (and, in turn, students) to use technology effectively in their classroom.

Planning and Implementing Professional Development

- Standards for Professional Learning, Learning Forward
- ISTE Standards for Teachers, International Society for Technology in Education

Student Data Privacy

School districts are trusted with sensitive student data. As good stewards of this data the SDM established a process for reviewing third-party software applications to ensure data is used only for educational purposes.

This Software Security, Privacy, and Safety Rubric (Appendix B) grades the software across seven key metrics. Reviewed online services are described in the SDM Online Reviewed Services (Appendix C) document. Any software product must be reviewed before student accounts are created or student data is shared.

Digital Learning Tools & Resources

Digital learning tools and resources include hardware, software, peripheral devices, and other tools used to create or support learning activities.

Software Basic Load

The basic load is the default software available on teacher devices.

Software	Notes	License Cost
Microsoft Windows 11 Professional	License typically included with new hardware. Windows 7 is phased out during the 2023-24 school year.	N/A Or $110.00
Google Chrome	Web browser	N/A
Mozilla Firefox	Web browser	N/A
Google Drive File Stream	Cloud file software	N/A
Adobe Acrobat Reader	PDF viewing software	N/A
Promethean	***Teachers with Promethean boards only*** Includes the latest version of Active Driver and Active Inspire. Licenses included with Promethean hardware.	N/A
Sharp Pen	***Teachers with Sharp Aquos boards only*** Includes the latest version of active pen software. License included with device.	N/A
HoverCam Flex	***Teachers with HoverCam document cameras only*** Latest version of HoverCam software.	N/A
IPEVO Presenter	***Teachers with IPEVO document Cameras only*** Latest version of IPEVO presenter software.	N/A
Microsoft Office	Office productivity software for Math teachers. Needed for equation notation features.	N/A

Specialized Software

Art Macintosh Lab Software

Software	Notes	License Cost
Adobe Photoshop Elements	Installed on all lab computers.	$72.00

Secondary Special Education Software

Software	**Notes**	**License Cost**
Bookshare	Online repository of accessible content. Only available to students with print disabilities. Available on Chrome OS and Windows.	N/A
Read2Go	iOS iPad application which integrates with Bookshare.	$20.00

Software Subscriptions

This is a list of software subscriptions available to staff & students.

Product	Description
Kami	Allows students to edit PDF files as part of assignments.
Pear Deck	Allows teachers to host interactive slideshow sessions with students.
Typing Tastic	Interactive typing lesson targeted to elementary students.
Edpuzzle	Innovative service allows teachers to wrap lessons around YouTube videos. Tracks if students watch video and prompts them for questions during video.
SeeSaw	Learning management system for elementary students.
Read&Write	Text to speech and speech to text tool for Chromebooks. Purchased for students with special needs. Available for all staff and students.
Buncee	Online content creation tool for teacher or student. Allows them to create interactive presentations
Other subscriptions may be available through the media center using library funds.	

Selecting and Evaluating Hardware, Software, and Devices

Teachers should have a voice in choosing their available tools. A selection committee will be able to provide valuable information about how software features will impact classrooms. An evaluation rubric customized to the specification of the committee should guide the selection process. Large purchases over $10,000 require a request for proposal (RFP) as part of the purchase process.

Any software used by students shall also meet district standards regarding student data privacy.

Teaching & Learning Support

Staff Communication

Incident & Problem Management

When a device or service does not work properly the end user contacts the help desk for assistance in resolving the issue. This issue is referred to as an ***incident*** and is tracked as a help desk ticket. A collection of related incidents is called a ***problem***. The technology director shall document problems, determine the scope in the schools, create and implement a plan to fix with the least amount of disruption.

- The technology directors engagement style is to be present in each building for some part of the day making regular check ins with key people in the district. (front desk personnel) as well as walking through the halls and checking with teachers on a daily basis

Technology Lifecycle Management

Staff Laptop Lifecycle

We target staff laptop updates every three to four years. I am working with various staff to determine the viability of using professional level Chromebooks as a replacement for Windows OS laptops. With a costs savings of over 50%. Staff scheduled to receive an updated laptop for the summer of 2022 is included in Appendix E. Every year we order extra devices to ensure replacement devices are available. Devices that have completed their standard duty cycle may be reused in other areas in the district.

Staff Desktop & Presentation Station Lifecycle

A presentation station is the technology used by a teacher to share information during class. This typically includes a computer, wall mounted display, a desktop display and other peripherals such as a document camera.

- Office desktop and classroom presentation stations computers should be updated every five to six years. This sheet describes the desktop and classroom presentation stations in our buildings. We are also extending the life cycle of these units with the use of SSDs
- Display screens and projectors should be replaced every five to seven years.

Student Device Lifecycle

Devices are assigned to each student. Students are assigned a device in grade K, 5, and 10. The pandemic has seen a change in Google's life cycle sequence. Historically it was 3 years and now is up to 8 years of support and updates. This will allow the school district to save money on refreshing old systems.

Switch and Virtual Environment Lifecycle

All network switching has been updated and configured to handle all wifi, telephony, and data requirements. After the updates there has been a significant drop in loss of wifi, telephony issues and network connection issues.

Windows Servers

Our Windows servers are 2008 and 2016. Both software platforms are End of Life (EOF) as such we are looking into replacement or moving all data into the cloud to avoid replacement costs and future upgrade issues.

Change Management

Technology is constantly changing in schools. We need controls to ensure changes are planned to minimally affect end users. Changes should also be well communicated to stakeholders through the ***Manawa Tech Info*** google classroom or district-wide emails.

Server Updates

Maintaining servers requires periodic updates and scheduled downtime. When possible, updates should be scheduled after Friday after 5:30pm or on weekends. All servers are inspected daily at 5:30 a.m. to ensure continuity of services. Emergency maintenance may be necessary. Any server updates which require downtime needs to be scheduled with staff to minimize negative effects. When possible, server restarts are scheduled during off hours.

Allowed Google Apps

Students are only allowed to install Google apps which have been pre-approved for student use. Staff and students may request apps to be installed by opening a help desk ticket. Applications which require students to create accounts or submit information are subject to the student privacy review before approval.

Allow or Block Website

Our network security infrastructure includes a firewall and web filter. These systems prevent students from accessing websites considered inappropriate or dangerous. Sometimes educational content is incorrectly blocked. Also, content which should be blocked is allowed. Staff and students are encouraged to contact the director of technology to suggest any website to block or unblock.

Network Operations

Goals

We have three main goals for network operations. First we need to improve our disaster recovery strategy. Second, key hardware and software systems need a maintenance plan. Finally, our network infrastructure needs to be thoroughly documented.

Strategy

Documentation

Detailed documentation of the network infrastructure is of critical importance. We will need several weeks to explore and document the existing systems. CESA has been invaluable in getting us started. Passwords are secured using a password management tool. CESA has access to this password management tool to ensure essential information is preserved.

Anti-Virus Protection

The SDM uses the Microsoft antivirus packages on Windows 10. Due to cyber insurance we will be looking to another antivirus package due to the changing nature of the cyber attack vectors.

Disaster Recovery

During the fall of 2021 we installed a new backup solution. This will greatly improve our redundancy. It will also allow us to "spin up " a compromised server in the cloud to maintain our continuity of services. At the request of the insurance company we are looking into encrypted and Write Once Read Many (WORM)/immutable backups.

Administrative Computing

School Website

We are in the process of OCR compliance and projected to have this completed by spring of 2023. This website is an important tool to share information with staff, students, and the greater community.

Account Automation

Students' accounts are automatically created or suspended based on their status in Skyward. This limits the risk of former students abusing Google accounts after leaving the district.

We are in the process of configuring Skyward to allow students and their families to register and enroll online. This process has been successful for the summer school 2022 session with a 95% utilization rate. This has reduced front office paper handling and data entry by significant margins. We are hoping to have this available for the fall 2022-2023 school year.

Internal controls automation with Skyward.
We are in the process of configuring Skyward to allow staff to generate various requests and reports without the intervention of a frontdesk employee. This will be an ongoing process as data demands change over time and thus the requests will change.

Planning & Budgeting

Staff Devices

- Teacher Laptops: 5-6 year replacement cycle
- Office Staff Desktops: 6 year replacement cycle

Student Devices

- The district needs to purchase about 50 devices annually to support the district-wide 1-to-1 Chromebook program.
- Computer Labs:
    - Engineering lab: This lab has been configured to allow for upgrades. So, we should be able to use the equipment for 5-7 years. Due to the cost we may need to stagger device replacement.
    - Mac Lab: These devices need to be on a 6-7 year replacement cycle. Due to the cost we may need to stagger device replacement. Due to cost and availability of computer chips we will be updating the existing hardware with SSD to get another 2 to 5 years in the life cycle of these systems.

Infrastructure

- Switches: Every switch has been updated and configured to be meet security compliance through 2028.
- Server Operating Systems: will be rebuilt or moved to the cloud by Fall semester of 2022
- WiFi Access Points: Access points will be upgraded during the 2023-24 school years as access points become available.
- Where possible we need to stagger expensive costs across multiple years.

References

Barnett, H. (2001). Successful K-12 technology planning: Ten essential elements. (ERIC Digest). Syracuse, NY: ERIC Clearinghouse on Information and Technology. (ERIC No. ED457858)

Stockert, Tim (2017). "How to Create a Technology Plan (Yes, You Need One)." Interpretation, 9 June 2017, www.coablog.org/home/2017/6/9/how-to-create-a-technology-plan.

Appendix A: Technology Acceptable Use and Safety Form

Electronic Version of Document

Appendix B: Software Security, Privacy, and Safety Rubric

Electronic Version of Document

Appendix C: SDM Online Reviewed Services

Electronic Version of Document

Students choosing to excel; realizing their strengths.

To: Mr. Ryan Peterson, Manawa Board of Education
From: Lance Litchfield
Date: 7/13/2023
Re: 2023-2024 Coaches Handbook Revisions

The purpose of this memo is to highlight the changes in the SDM Coaches Handbook as follows:

Page #	***Current Language (If applicable.)***	***Proposed Change or Addition***
6	Each coach, paid and volunteer, will complete the professional development course through the 3D Institute two weeks prior to the start of their season. This course will provide each coach with a certificate upon completion to turn into the Athletic Director. A positive culture is an essential base to be successful in competition, in our schools, and in our communities. This course will unify our athletic department in a movement of a positive culture.	~~Each coach, paid and volunteer, will complete the professional development course through the 3D Institute two weeks prior to the start of their season. This course will provide each coach with a certificate upon completion to turn into the Athletic Director.~~ ~~A positive culture is an essential base to be successful in competition, in our schools, and in our communities. This course will unify our athletic department in a movement of a positive culture.~~ All head and assistant coaches at any level are encouraged to attend at least one coaching clinic per year. One clinic per year per coaching staff, will be paid for by the Athletic Department. If a coach does not attend a clinic however, it is an expectation that they do something else in the off-season to improve their coaching ability. Additionally, all head and assistant coaches can attend one clinic, per sport s/he coaches, during that school year. All coaching days need to be cleared through the athletic department.
7	**Will be titled "Culture Training"** Head Coaches will use their training through the 3D Institute, its resources,	~~CULTURE TRAINING~~ ~~Head Coaches will use their training through the 3D Institute, its resources,~~

	and the athletic director to have culture lessons for thirty minutes each week of their sports season. These lessons will focus on the skills and characteristics of highly successful individuals. Lessons can be added into practice time or be separate from the practice format. Ideally, coaches would utilize a designated classroom to instruct, discuss, and lead a cultural change on their team and in the athletic department of the School District of Manawa.	~~and the athletic director to have culture lessons for thirty minutes each week of their sports season. These lessons will focus on the skills and characteristics of highly successful individuals. Lessons can be added into practice time or be separate from the practice format. Ideally, coaches would utilize a designated classroom to instruct, discuss, and lead a cultural change on their team and in the athletic department of the School District of Manawa.~~
7	Head Coaches will be evaluated on a yearly basis using the 3D Institute model for professional development. The Head Coach will work with the Athletic Director to evaluate assistant coaches, with a recommendation whether to rehire to the Athletic Director.	Head Coaches will be evaluated on a yearly basis by the Athletic Director ~~using the 3D Institute model for professional development~~ by the Athletic Director. The Head Coach will work with the Athletic Director to evaluate assistant coaches with a recommendation whether to rehire to the Athletic Director.

The Little Wolf High School Student Handbook will be posted to the School District of Manawa website following Board of Education approval of substantive language changes as presented. The Manawa Board of Education will be notified of the date that this handbook (or plan as appropriate) is converted to a version considered compatible for use by individuals with visual impairments or limited vision as per the Office of Civil Rights requirements and posted to the School District of Manawa website. This OCR compatible conversion may impact the appearance of the document (i.e. change in fonts, font sizes, paging in the table of contents, etc.) resulting in technical changes but no substantive changes will be made. Should a substantive change be required, the handbook (plan) will be brought back to the Board of Education for approval.

CYBER INCIDENT RESPONSE PLAN

Updated: July 2023

Abstract
Our working definition of a cyber incident is any violation (or imminent threat of violation) of computer security policies or standard security practices that has significant potential to lead to negative impact to the district's reputation, inappropriate access to student or financial data, and/or loss of intellectual property or funds.

School District of Manawa Cyber Incident Response Plan

Introduction

All security incidents must be managed in an efficient and time effective manner to make sure that the impact of an incident is contained and the consequences to the school district are limited. This document sets out the School District of Manawa plan for reporting and dealing with security incidents.

What is a Security Incident?

A Security Incident means any incident that occurs by accident or deliberately that impacts your communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services. This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by the School District of Manawa.

How to Recognize a Security Incident

A security incident may not be recognized straightaway; however, there may be indicators of a security breach, system compromise, unauthorized activity, or signs of misuse within our environment, or that of third-party service providers.
District staff need to watch for any indications that a security incident has occurred or may be in progress, some of which are outlined below:

- Monitor excessive or unusual log-in and system activity, in particular from any inactive user IDs (user accounts)
- Watch out for excessive or unusual remote access activity into your business. This could be relating to staff or third-party providers
- The occurrence of any new wireless (Wi-Fi) networks visible or accessible from the district environment
- The presence of or unusual activity in relation to malware (malicious software), suspicious files, or new/unapproved executables and programs. This could be on district networks or systems and includes web-facing systems.
- Hardware or software key loggers found connected to or installed on systems
- Suspicious or unusual activity on, or behavior of, Web-facing systems, such on as ecommerce website

- Point-of-Sale (POS) payment devices, payment terminals, chip & PIN/signature devices or dip/swipe card readers showing signs of tampering
- Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain district financial, student or other sensitive data

The cyber incident response plan must be followed by all personnel in the district. This includes all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of the School District of Manawa, working with the district's data or on SDM premises. For simplicity, all these personnel are referred to as 'staff' within this plan.
Roles

The SDM Cyber Incident Response Team (CIRT) is comprised of:
Role* CIRT Responsibility Name Email Telephone Director of Technology Incident Response Lead Dmarzofka@manawaschools.org 920-592-2525
Director of IT

Primary Risk Owner
District Administrator
Ryan Peterson
RPeterson@manawaschools.org 920-592-5300

The District Administrator will be the Director of Communications Handling of any external communications in relation to security incidents and for the handling of any personnel and disciplinary issues relating to security incidents Staff Attorney Handling of any legal questions / issues relating to security incidents. Building principals – Teaching & Learning Handling of potential disruption of school operations detailed responsibilities

The Incident Response Lead is responsible for:
- Making sure that your Cyber Incident Response Plan and associated response and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.
- Making sure that the Cyber Incident Response Plan is up to date, reviewed and tested at least once each year.
- Making sure that staff with Cyber Incident Response Plan responsibilities are properly trained, at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Cyber Incident Response Plan, as and when needed.
- Reporting to and liaising with external parties, legal representation, law enforcement, etc. as is required.
- Authorizing on-site investigations by appropriate law enforcement, insurance company security / forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.
- Cyber Incident Response Team (CIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected security incident.
- Advising the Incident Response Lead of an incident when they receive a incident report from staff.
- Investigating each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Reporting each security incident and findings to the appropriate parties. This may include the third-party service providers, business partners, staff, parents, etc., as required.
- Assisting law enforcement and industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
- Resolving each incident to the satisfaction of all parties involved, including external parties.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.
- All staff members are responsible for:
- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Cyber Incident Response Team (CIRT).
- Reporting any security related issues or concerns to line management, or to a member of the CIRT.
- Complying with the security policies and procedures of the School District of Manawa. This includes any updated or temporary measures introduced in response to a security incident (e.g. for business continuity, incident recovery or to prevent recurrence of an incident).

External Contacts

Incident Response Plan Steps

Best practice for responding to security incidents indicate specific actions that must be taken to ensure that the district is protected.

1. Information security incidents must be reported, without delay, to the Incident Response Lead (preferable) or to another member of the Cyber Incident Response Team (CIRT). The member of the CIRT receiving the report will advise the Incident Response Lead of the incident.
When a potential incident is discovered, the team should immediately collect additional evidence, decide on the type and severity of the incident, and document everything they are doing. Documentation should answer “Who, What, Where, Why, and How” questions to allow the attackers to be prosecuted in court at a later stage. External Party Contact Name Email

Telephone:
In this order:

1. SDM Cyber Insurance Company 262-252-6546
2. State of Wisconsin Cyber-response-teams.aspx 800-943-0003 Wisconsin Statewide Intelligence Center (WSIC) / Fusion Center On-call wsic@doj.state.wi.us Click on “Report Cyber Incident”: https://wifusion.org 888-324-9742
3. FBI Internet Crime Complaint Center (IC3) Online File a complaint: https://www.ic3.gov/default.aspx
4. Waupaca County Sheriff’s Office

2. After being notified of a security incident, the CIRT will perform an initial investigation and determine the appropriate response, which may be to initiate the Cyber Incident Response Plan. If the Security Incident Response Plan is initiated, the CIRT will investigate the incident and initiate actions to limit the exposure of district data and in mitigating the risks associated with the incident.
Initial incident containment and response actions

- Isolate compromised systems from the network and unplug any network cables – without turning the systems off.
- If using a wireless network, change the SSID (Service Set Identifier) on the wireless access point and other systems that may be using this wireless network (but not on any of the systems believed to be compromised).
- Preserve all logs and similar electronic evidence, e.g. logs from firewall, anti-virus tool, access control system, web server, application server, database, VPN, application servers, etc.
- Perform a back-up of systems to preserve their current state – this will also facilitate any subsequent investigations (after verifying with forensic team).
- Keep a record of all action’s members of the CIRT take in regard to the event.
- Stay alert for further indications of compromise or suspicious activity in the district environment, or that of third parties.
- If possible, gather details of all compromised or potentially compromised systems.

Once the CIRT has carried out their initial investigation of the security incident and determined that the Cyber Incident Response Plan is to be activated:

3. The Incident Response Lead will alert the CIRT's senior management primary contact and open a communication method (currently Microsoft Teams) for all team discussion and activity recording.
4. The Incident Response Lead and / or the CIRT personnel responsible for communications / PR will inform all relevant parties. This may include insurance carriers and local law enforcement, and other parties that may be affected by the compromise such as staff, students, parents, business partners or suppliers. This also includes the personal data breach notification contacts, as applicable to the incident under investigation. **Use insurance company approved vendors if calling for outside forensic assistance.
Maintain Business Continuity

5. The CIRT will engage with school and operations departments to ensure the district can continue to operate while the security incident is being investigated.

- Verify that system and data backups are available in the event of loss of data, system corruption/virus infection or hardware failure.
- Consider what offline or alternative methods for continuing district operations (both teaching & learning and operational areas) will be used if district technology and/or internet access is not available.

6. The CIRT will liaise with external parties, including insurance company agents, law enforcement, etc., to ensure appropriate incident investigation (which may include on-site forensic investigation) and gathering of evidence, as is required.

7. The members of the CIRT will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational.

8. The Incident Response Lead will report the investigation findings and resolution of the security incident to the appropriate parties and stakeholders (including the school board, local law enforcement, etc.) as is needed.
Recovery

9. The Incident Response Lead will authorize a return to normal operations once satisfactory resolution is confirmed.

10. The CIRT will notify the rest of the business that normal business operations can resume. Normal operations must adopt any updated processes, technologies or security measures identified and implemented during incident resolution.

11. The CIRT Executive Officer/Risk Owner (the senior management primary contact) will ensure that the required updates and changes are adopted or implemented as necessary. The CIRT will complete a post-incident review after every security incident. The review should be performed no later than two weeks from the end of the incident and will consider how the incident occurred, what the root causes were and how well the incident was handled. This will

help to identify recommendations for better future responses and to avoid a similar incident in the future.
Changes and updates that may be required include:

- Updates to the Cyber Incident Response Plan and associated procedures.
- Updates to the district's security or operational policies and procedures.
- Updates to technologies, security measures or controls (for example, changes to data access or removal of applications with security issues)
- The introduction of additional safeguards in the environment where the incident occurred (for example, more effective malware protection).

Appendix A

Specific Incident Response Types
Some specific incident types requiring additional response actions are provided below.
Malware (or Malicious Code)

1. Disconnect devices identified with malware from the network immediately.
2. Examine the malware to identify the type (e.g. rootkit, ransomware, etc.) and establish how it infected the device. This will help you to understand how to remove it from the device.
3. Once the malware has been removed a full system scan must be performed using the most up-to-date signatures available, to verify it has been removed from the device.
4. If the malware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by the malware.
5. Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.

Unauthorized Wireless Access Points

If unauthorized wireless access points are detected, or reported by staff, these must be recorded as a security incident.

1. CIRT will investigate to identify the location of the unauthorized wireless access point/device.
2. The CIRT will investigate as to whether the unauthorized wireless access point/device is being used for a legitimate district purpose/need. If a legitimate reason is identified, then this wireless access point or device must be reviewed and go through the correct management approval process. This is to make sure that the justification is documented, and the wireless access point/device is securely configured (e.g. change default passwords and settings, enable strong authentication and encryption, etc.).
3. All other unauthorized wireless access points/devices must be located, shutdown and removed.

Loss of Equipment

1. The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to a member of the CIRT and local law enforcement. This includes losses/thefts outside of business hours and at weekends.
2. If the device that is lost or stolen may have contained sensitive data, and the device is not encrypted, CIRT will complete an analysis of the sensitivity, type and volume of data stolen.
3. Where possible, CIRT will use available technology/software to lock down/disable lost or stolen mobile devices (e.g. smart phones, tablets, laptops, etc.) and initiate a remote wipe. Evidence should be captured to confirm this was successfully completed.

Non-Compliance with Security Policy

1. This covers incidents resulting from deliberate or accidental actions that are in breach of your security policy and which put student or financial data at risk. This includes any systems or data misuse, unauthorized exposure of data to external parties, unauthorized changes to systems or data.
2. CIRT will engage with the relevant school / department to establish an audit trail of events and actions. They will determine who is involved in the policy violation and the extent of the violation.
3. CIRT and/or building administrators will notify Human Resources of the incident.
4. CIRT will liaise with Human Resources to determine whether disciplinary action is needed.
5. CIRT will undertake an assessment of the impact and provide advice and guidance to the school / department to prevent recurrence, for example re-training of staff.

Appendix B
Testing and Updates

Annual testing of the Cyber Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the CIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually.
2. The Incident Response Plan Testing will test district response to potential incident scenarios to identify process gaps and improvement areas.
3. The CIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to CIRT members.

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed

manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in -- either virtually or for real -- and reporting back the findings.

The School District of Manawa shall perform pen testing regularly (ideally once a year) to ensure our data environment, network security and procedures are consistent and adequate. In addition, tests may also be conducted when the district:

- adds new infrastructure or applications
- makes significant upgrades or modifications to existing infrastructure
- adds an additional location to the wide-area network
- applies security patches or fixes
- makes a significant change to end user security policies

Some of the pen testing needs may be completed by cloud partners of the district;

- The district will make every effort to participate in security organizations that provide testing benefits to members such as MS-ISAC and WI-CRT.
- https://searchsecurity.techtarget.com/definition/penetration-testing

Appendix C
Network diagrams & server usage
Current network diagrams and listing of servers (with designated use) are necessary for determining where and how cyber incidents occur. The following pages outline our network switches, servers, fiber strand and wireless SSID setups. Pictures of all district wiring closets are stored on the tech department shared drive.

Appendix D
District Security and Backup Practices
The School District of Manawa strives to follow best practice for data security, student privacy, and network operations. The following items are updated as best practices evolve and change. This section of the CIPR will be updated at least once per year.

Data retention
(Student records) contains the district's practice regarding student records and data retention. The following links are to the Wisconsin Department of Public Instruction's guidance regarding student data and retention.
https://dpi.wi.gov/rl3/records
https://publicrecordsboard.wi.gov/Documents/DPI%20GS-APPROVED%20June%202015%20v8.1.pdf

Authentication practices
District policies regarding passwords and authentication are being revised for the 2022-23 school year. Student passwords will require complex password structures for grades 6-12 and students will have a portal for changing their passwords. With this change in practice, only

grades 4K-5 will have user password information saved on Skyward (for staff use to assist in logins).
The National Institute for Standards and Technology (NIST) has updated their guidelines for password management practices to include the following 4 areas: Complex passwords that have been checked against known leaked breach data and known weak passwords, password lengths beyond 8 characters and up to 64 characters, no hint questions for password resets, and ending the practice of regular password changes.
For the 23-24 school year, the district will require staff to change their passwords and will give them tools to check their password before using it. All efforts will be made to work with current AD authentication to adopt the NIST recommendations, including activating the "Risky Login" feature in AD. The district will also require multi-factor authentication for any user with direct access to the financial server data stores (Skyward PAC users).

User access practices
All district accounts are based on the premise of "least privileged user access" when created. The district has done multiple reviews of user accounts to remove administrator level access from users who do not need full rights to complete their assigned duties. For certain staff, the technology team has provided the ability to "run as admin" from a specific machine to complete local administration tasks on computer labs, etc. See https://www.beyondtrust.com/resources/glossary/least-privilege for a further description of least privilege.
Additionally, the district uses cloud monitoring software to automatically review online apps or systems that users may install using their manawaschools.org addresses. This process (currently done by ManagedMethods) allows for the district to rescind and block access to user level data for applications that are not secure and/or are not approved for use within the district domain.

Student take-home use of district devices
With the district focus on personalized learning, students in grades 6-12 have access to district-owned computing devices (Windows laptops, Chromebooks) for use outside of the school network. To provide a safe environment on these devices, the district uses GoGuardian to provide monitoring of student activity when not on the district network. GoGuardian provides a parent portal where parents can restrict student use on those devices beyond the CIPA (Child Internet Protection Act) required filtering that the district enforces. Parents are provided an account which can be used to allow or deny additional content categories. Bark is used as a backup to Securly, and those alerts are sent to district staff for review.

Data backup practices
As of 2022, the district is migrating backup processing from local Unitrends appliances to Veeam server-based backups pushing to Arcserver in the cloud. This upgrade will allow the district to use existing storage more efficiently and allow for the expansion of backup processes to include an automated off-site backup to co-located equipment housed in the Waukesha School District data center. Appendix C contains the current backup location and frequency of all district servers.

Network firewall configuration practices
For security reasons, the district firewall configuration is not documented in this plan. A copy of the configuration is backed up as part of the normal district backup practices.

User Identity Management practices
The district is in the process of automating user account provisioning and deprovisioning. The authoritative source for student accounts is Skyward. When student enrollments are created or ended in Skyward, will make changes to the student Active Directory accounts as needed. The district is in the testing stages for staff account creation and deprovision based on the Skyward Human Resources server. Once completed, OneSync will be used for all staff accounts as well.

Remote wipe of district devices (if lost or stolen)
The district currently can lock and wipe all Chromebooks and Apple devices.

School District of Manawa Students

Choosing to Excel, Realizing Their Strengths

Employee On-Boarding

Name: _____ **Position:** _____

Steps to Complete	Date Completed
BACKGROUND CHECK form: Received _____ Started _____ *(Admin Assist)* Initial when completed:_____	
Send ThedaCare at Work pdf file to Employee with employees Job Description *(Admin Assist)* Initial when completed:_____ Date of Appointment: _____	
Board of Education Approval Date: _____	
Contract or MOU prepared and sent to Employee *(HR):* Initial when completed:_____	
Payroll Paperwork to Employee: Emailed / picked up (Circle one) _____ *(Business Office)* Initial when returned:_____	
Create Employee Personnel file / create payroll file *(HR/Business Office)* Initial when completed:_____	
Copy of License(s) and Resume on File *(Business Office)* Initial when completed:_____	
Explain Time Off Process and refer to Handbook (rules) *(HR)* Initial when completed:_____ Signature Page Returned: _____	
For Hourly Paid Staff - Explain the time card process for payroll; where to get the cards *(Business Office)* Initial when completed:_____	
Email Technology Acceptable Use Packet to Employee *(HR)* Initial when completed:_____	
Request IT to set up email for new hire *(Business Office)* Initial when completed:_____	

Email the Mandatory Reporting and Required Training to new hire *(HR)* **Initial when completed:_____** ● **Annual Presentation for Pupil Services 2023 - Completed: _____** ● **Bloodborne Pathogens School Training - Completed: _____** ● **Civil Rights ? Completed: _____** ● **Mandatory Reporting of Child Abuse and Neglect Training (All School Employees) - Completed: _____** ● **Mandatory Reporting of Threats of School Violence - Completed: _____** ● **Annual Signature From Teachers and Staff 2023-2024 - Completed: _____** ● **Title IX - Completed: _____** ● **ALICE Training - Completed: _____** ● **Personal Identifiable Records - Completed: _____**	
Required Policies: (In Progress) ●	
Sub-Training: (In Progress) ●	
Employee Shirt - sizing. *(Admin Assist)* Initial when completed:_____	
Keys and Fob check out / form signed / Brivo and ISONAS updated *(Admin Assist)* **Initial when completed:_____**	
If hired after Inservice use "Mid-School Hire OnBoarding Checklist" (In Progress)	

School District of Manawa Students

Choosing to Excel, Realizing Their Strengths

To Prospective Employees and Volunteers:

This form is intended for the safety of our community and our children. As a prospective employee or volunteer for the School District of Manawa we would appreciate the opportunity to ask our Police Department and the Dept. of Justice to run a background check. All information will be confidential between the Police Department and the Administration of the Manawa School District. Any information received will be shared with the applicant upon request.

Please indicate your consent with full signature below:

_____ _____

SIGNATURE TODAY'S DATE

Please print legibly your Full Legal Name below:

First:_____ Middle:_____ Last: _____

ALL Previous Names: _____

Currentt Address: _____

Previous Address: _____

Previous Address: _____

Previous Out-of-State Addresses: _____

Have you lived outside of the United States within the last 10 (ten) years? Yes/No (Circle one).

Have you ever been convicted of a felony? Yes ___ No ___

If yes, explain: _____

DOB: _____ Gender: Male ___ Female ___

Race:White ___ Asian ___ Black ___ Hispanic ___ American Indian/Alaskan ___ Haw/Pacific Islander ___

Current email address and phone number: _____

Thank you for your cooperation!

School District of Manawa
800 Beech Street
Manawa, WI 54949
Phone: (920) 596-2525
Fax: (920) 596-5308
District Administrator: Ryan M. Peterson

Little Wolf High School
Manawa Middle School
515 E. Fourth St
Manawa, WI 54949
Phone: (920) 596-5800
Fax: (920) 596-2655
Principal: Michelle Johnson

Manawa Elementary
800 Beech Street
Manawa, WI 54949
Phone: (920) 596-5700
Fax: (920) 596-5308
Principal: Danni Brauer

ManawaSchools.org

/ ManawaSchools

/ ManawaSchools

DISCLOSURE AND AUTHORIZATION FORM TO OBTAIN CONSUMER REPORTS

Please Read Carefully Before Signing the Authorization

DISCLOSURE

In considering you for volunteer and, if you are employed, in considering you for subsequent promotion, assignment, reassignment, retention, or discipline, the School District of Manawa ("the Company") may request and rely upon one or more consumer reports or investigative consumer reports about you that we obtain from a consumer reporting agency, such as IntelliCorp Records, Inc.

For explanation purposes:

- A "consumer report" is a written, oral or other communication of any information by a consumer reporting agency bearing on your credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in making a volunteer-related decision about you. Such information may include, for example, credit information, criminal history reports, or driving records; and
- An "investigative consumer report" is a consumer report in which information on your character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with your prior employers, neighbors, friends, or associates, or with others who may have knowledge concerning any such items of information. In the event an investigative consumer report is request about you, you are entitled to additional disclosures regarding the nature and scope of the investigation requested, as well as a written summary of your rights under the Fair Credit Reporting Act ("FCRA").

Under FRCA, before the Company can obtain a consumer report or investigative consumer report about you for volunteer purposes, we must have your written authorization. Before we take adverse action on the basis, in whole or in part, of information in that report, you will be provided a copy of that report, the name, address, and telephone number of the consumer reporting agency, and a summary of your rights under the FRCA.
https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf

School District of Manawa

"Students Choosing to Excel, Realizing Their Strengths"

ANNUAL REQUIRED NOTICES

CONFIDENTIALITY AGREEMENT

To the extent permitted and/or required by law, as a staff member or volunteer for the School District of Manawa, I **will not** disclose any information I hear or receive in written form, referencing a School District of Manawa student, staff member, parent and/or potential/existing volunteer to anyone except to legally authorized persons including law enforcement officials and/or the administrator in charge (Principal/District Administrator).

ACCEPTABLE USE AGREEMENT

I have received, read, understand, and will abide by the School District of Manawa's *Acceptable Use Agreement* when using a computer and other electronic resources owned, leased or operated by the School District of Manawa. I further understand that any violation of the regulations listed in this policy is unethical and may constitute a criminal office. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated. Additional copies of the agreement can be found in building offices.

TECHNOLOGY ACCEPTABLE USE AND SAFETY FORM

I have read and understand the *Technology Acceptable Use and Safety Form*. I understand that unauthorized or inappropriate use, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action and/or civil criminal liability (see Sec. 943.70, Wis. Stat. (Computer Crimes), Sec. 947.0125, Wis. Stat. (Unlawful Use of Computerized Communication Systems)).

Complete this agreement form and submit it to the school/district office. My signature signifies that I understand and agree to abide by this agreement regarding all information in the document.

PRINT NAME: _____ DATE: _____

SIGNATURE: _____

Technology Acceptable Use and Safety Form

Staff Form

Staff members are authorized to use the Board of Education's computers, laptops, tablets, personal communication devices (as defined by Policy 7530.02), network, and Internet connection and online educational services ("Education Technology" or "EdTech") for educational and professional purposes. Use of Education Technology is a privilege, not a right. Staff members must conduct themselves in a responsible, efficient, ethical, and legal manner. Unauthorized or inappropriate use, including any violation of these guidelines, may result in cancellation of the privilege, disciplinary action and/or civil criminal liability (see Sec. 943.70, Wis. Stat. (Computer Crimes), Sec. 947.0125, Wis. Stat. (Unlawful Use of Computerized Communication Systems)). Prior to accessing the Education Technology, staff members must sign the Staff Education Technology Acceptable Use and Safety Agreement. Staff members must complete mandatory annual training.

Smooth operation of the Board's Education Technology relies upon users adhering to the following guidelines. The guidelines outlined below are provided so that users are aware of their responsibilities.

A. Staff members are responsible for their behavior and communication using the Ed-Tech. All use of the Education Technology must be consistent with the educational mission and goals of the District.

B. Staff members may only access and use the Education Technology by using their assigned account and may only send school-related electronic communications using their District-assigned email addresses. Use of another person's account/e-mail address/password is prohibited. Staff members may not allow other users to utilize their passwords. Staff members may not go beyond their authorized access. Staff members are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers/laptops/tablets/personal communication devices when leaving them unattended.

C. Staff members may not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, or misrepresent other users on the District’s network. Staff members may not intentionally disable any security features of the Ed-Tech.

D. Staff members may not use the Education Technology to engage in "hacking" or other illegal activities (e.g., software pirating, intellectual property violations; engaging in slander, libel or harassment; threatening the life or safety of another; stalking;

transmission of obscene materials or child pornography, including sexting; fraud; sale of illegal substances or goods.

1. Slander and libel are terms defined specifically in law. Generally, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by

2. Houghton Mifflin Company. All rights reserved.) Staff members shall not knowingly or recklessly post false or defamatory information about a person or organization. Staff members are reminded that material distributed over the Internet is "public" to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people and harmful and false statements will be viewed in that light.

3. Staff members shall not use the Education Technology to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation or transgender identity, age, disability, religion or political beliefs. Sending, sharing, viewing or possessing pictures, text messages, e-mails or other materials of a sexual nature (i.e., sexting) in electronic or any other form, including the contents of a personal communication device or other electronic equipment, is grounds for discipline, up to and including termination. Such actions will be reported to local law enforcement and child services as required by law.

E. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.

F. Any use of the Ed-Tech for commercial purposes, advertising, or political lobbying is prohibited.

G. Staff members are expected to abide by the following generally accepted rules of online etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the

Board's Education Technology. Refrain from using obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.

2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.

3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a staff member is told by a person to stop sending him/her messages, the staff member must stop.

4. Do not post information that, if acted upon, could cause damage or danger of disruption.

5. Never reveal names, addresses, phone numbers, or passwords of students while communicating on the Education Technology, unless there is prior written parental approval or it is otherwise permitted by Federal and/or State law.

6. Check email, at least daily per employee handbooks. Nothing herein alters the staff member's responsibility to preserve e-mail and other electronically stored information that constitutes a public record, student education record and/or a record subject to a Litigation Hold.

H. Use of the Education Technology to access, process, distribute, display, or print child pornography and other material which is obscene, objectionable, inappropriate or harmful to minors are prohibited. For example, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that depicts, describes, or represents in a patently offensive way with respect or what is suitable for minors an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals, and material that lacks serious literary, artistic, political, or scientific value as to minors. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the Board's computers/network (e.g., viruses) are also prohibited.

   To ensure that the Board's computer resources are not used for inappropriate purposes and consistent with the Children's Internet Protection Act, the Board has implemented technology protection measures on all computers with Internet access that protect against access to visual depictions that are obscene, child pornography, and/or harmful to minors. These measures are operating at all times, and enable the Board to monitor and protect against access to the aforementioned visual depictions. We have additional and extensive systems and security mechanisms in place to ensure the security, integrity, and appropriateness of the data on our networks. We

also rely on and respect each family's right to decide whether to allow their children access to the Internet.

I. Malicious use of the Board's Education Technology to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system is prohibited. Staff members may not engage in vandalism or use the Ed-Tech in such a way that would disrupt its use by others. Vandalism is defined as any malicious or intentional attempt to harm, steal or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass Network security and/or the Board's technology protection measures. Staff members may not use the Board's Ed-Tech in such a way that would disrupt their use by others. Staff members should refrain from intentionally wasting limited resources.

J. All communications and information accessible online should be assumed to be private property (i.e, copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions of authorship must be respected.

K. Downloading of information onto school-owned equipment or contracted online education services is prohibited, without prior approval from the Technology Director. If a staff member transfers files from information services and electronic bulletin board services, the staff member must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a staff member transfers a file or software program that infects the District’s Ed-Tech with a virus and causes damage, the staff member will be liable for any and all repair costs to make the Education Technology once again fully operational.

L. Staff members have no right or expectation to privacy when using the Education Technology. The District reserves the right to access and inspect any facet of the Ed-Tech, including, but not limited to, computers, laptops, tablets, personal communication devices, networks or Internet connections or online education services, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein. A staff member's use of the Ed-Tech constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the EdTech and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead

to a discovery that a staff member has violated Board policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a staff member has violated Board policy and/or law, or if requested by local, State or Federal law enforcement officials. Staff is reminded that their communication is subject to Wisconsin's public records laws and FERPA (See Policy 8330). The use of passwords does not guarantee confidentiality, and the Board retains the right to access information in spite of a password.

M. Use of the Internet and any information procured from the Internet is at the staff member's own risk. The Board is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions. The Board is not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from Internet sources used in class should be cited the same as references to printed materials. The Board is not responsible for financial obligations arising through the unauthorized use of the Ed-Tech. Staff members will indemnify and hold the Board harmless from any losses sustained as the result of misuse of the Ed-Tech by the staff member.

N. Disclosure, use and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent on the "Student Education Technology Acceptable Use and Safety Agreement Form."

O. Proprietary rights in the design of websites hosted on the Board-owned District-affiliated or leased servers remains at all times with the Board without prior written authorization.

Staff members are required to limit student exposure to commercial advertising and product promotion when developing the District or classroom websites or giving other assignments that utilize the Internet. Under all circumstances, staff members must comply with COPPA.

Staff members are reminded that personally identifiable student information is confidential and may not be disclosed without prior written parental permission.

Please Note Meal Allowance for employees approved to stay overnight for conference / workshop / meetings is $9 for Breakfast, $10 for Lunch, $16 for Dinner. Employees will only be reimbursed for the above amounts. Please attach all itemized meal receipts to the back of this form.**

SCHOOL DISTRICT OF MANAWA
Mileage Rate Updated 1/1/2021 23

EXPENSE AND MILEAGE REIMBURSEMENT

Name: _____

INSTRUCTIONS: See meal allowances above and mileage info below. **Support all items claimed.** See mileage table below. Submit as soon as possible to your building principal / supervisor for approval. Attach all detail receipts to the back of this form.

Date	Explanation	# miles	Total Expenses

_____
Bldg. Administrator's Approval

_____
District Administrator's Approval

_____

Account # _____

# of miles _____
x ~~.56 / mile~~ $0.655 (1/1/2023)
Mileage Total $_____
Plus Expenses $_____
Requested Amt $_____

Mileage from Manawa to: (round trip) If your destination isn't listed, set your trip meter!
Your reimbursement will be for mileage listed below or from trip meter – whichever is lower. If more than one employee is attending the conference, workshop or meeting you must carpool or use the District Van.

New London 24	Weyauwega 25	Waupaca 30	Wis. Dells 210
Iola 32	Clintonville 36	Marion 38	Neenah 88
Shawano 75	Appleton 70	Stevens Point 80	Eau Claire 300
Oshkosh 100	Wis. Rapids 100	Green Bay 116	Milwaukee 260
Wausau 130	Fond du Lac 140	Madison 250	

School District of Manawa
Meal Reimbursement
Effective 8/14/08

You may be reimbursed for meals if:

You are staying overnight
- attach detail meal receipt to green reimbursement form

See reimbursable meal amount limits on the front top of this form.

If you have any questions, please feel free to contact one of the following regarding this issue:

Carmen O'Brien
Business Manager
School District of Manawa

Julie Prey
Payroll / Accounts Payable
School District of Manawa

SCHOOL DISTRICT OF MANAWA
Mileage Rate Updated 1/1/2023

MILEAGE REIMBURSEMENT

Name:_____

INSTRUCTIONS: Support all items claimed. See mileage table below. Submit as soon as possible to your building principal/supervisor for approval. Attach all detailed receipts to the back of this form.

Date	Explanation	# Miles	Total Expenses

_____
Building Administrator's Approval

_____
District Administrator's Approval

Account #_____

# of miles_____
_____ x $.655

Mileage Total $_____

Requested Amt $_____

Mileage from Manawa to: (round trip) If your destination isn't listed, set your trip meter!
Your reimbursement will be for mileage listed below or from trip meter - whichever is lower. If more than one employee is attending the conference, workshop or meeting you must carpool or use the District Van.

New London 24	Weyauwega 35	Waupaca 30	WI Dells 210
Iola 32	Clintonville 36	Marion 38	Neenah 88
Shawano 75	Appleton 70	Stevens Point 80	Eau Claire 300
Oshkosh 100	WI Rapids 100	Green Bay 116	Milwaukee 260
Wausau 130	Fond du Lac 140	Madison 250	

Please Note**Meal Allowance for employees approved to stay overnight for conference/workshop/meetings is $9 for Breakfast, $10 for Lunch, and $16 for Dinner. Employees will only be reimbursed for the above amounts. Please attach receipts to the back of this form.

SCHOOL DISTRICT OF MANAWA
EXPENSE/MEAL REIMBURSEMENT(Non-mileage)

Name:_____

INSTRUCTIONS: See meal allowances above.Support all items claimed. Submit as soon as possible to your building principal/supervisor for approval. Attach all detailed receipts to the back of this form.

Date	Explanation	Total Expenses

_____
Building Administrator's Approval

_____
District Administrator's Approval

Expenses $_____
Requested Amt $_____

Account #_____