Oneida SD Technology Plan

Purpose:

The purpose of the technology resources of the Oneida School District is to support and promote student learning. Our Technology Plan is considered in terms of supporting that end goal. The action steps to achieve that goal are as follows:

1. Students:
    a. Keyboarding skills formally beginning at third grade
    b. Academic intervention support and academic support such as:
        i. I-Ready
        ii. IStation
        iii. Imagine Math
        iv. Edmentum
        v. Discovery Education
        vi. IXL Science
        vii. Pearson ELA
    c. Internet skills that support curricular enhancement, quality analysis of information skills, and specialized applications.
    d. Digital citizenship
    e. Workforce skill development
    f. Online learning (courses)
2. Parents:
    a. Instant access to students' progress, grades, attendance, tests, and assignments
    b. Access to district and school information and announcements
    c. Access to teachers
3. Teachers, Administrators, and Support Staff:
    a. Curriculum enhancement and support
    b. Provide student information to students and parents
    c. Record keeping, reports, and data management
    d. Professional development
4. District managed resources and infrastructure
    a. Provide technology access, security, and support
    b. Provide technologies to support above action steps
    c. Provide Professional development

Technology Committee:

It is best practice to meet annually with a committee of teachers, administrators, and other stake holders to update the plan and discuss: Ethics, technology curriculum, technology to assess, online resources, student information systems, and how technology can better be used to meet students learning needs.

Acceptable Use:

The Oneida School District uses the most efficient methods in the industry to protect users from inappropriate material. However, it is impossible to control all materials, and users may come across controversial or inappropriate information. We believe that the educational opportunities far outweigh the possibility that users may obtain objectionable material.

The burden of appropriate use falls upon the individual user. Specific details or appropriate use are covered in detail in the "Acceptable Use Agreement". All users of technology in the Oneida School District must sign this form and are held to these standards. The district reserves the right to restrict access to any given individual. The standards outlined on the "Acceptable Use Agreement" are strictly enforced. Violation of any of these standards can result in suspension, denied use, or termination of employment.

Acceptable Use Agreements

Acceptable Use Policy For Employees

Definition: Computer Network Communications include, but are not limited to, the use of local area networks, wide area networks, Internet, on-line commercial communications and all other commuter communications provided by or through the Oneida School District.

Conditions of Acceptable Use:

With access to computers and people all over the world also comes the availability of material that may not be considered to be of appropriate educational value in the context of the school setting. Oneida School District has taken precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies on the proper conduct of the end users who must adhere to strict guidelines. The following guidelines are provided so that you are aware of the responsibilities you are about to accept. In general, this requires efficient, ethical and legal utilization of the network and Internet resources. If an Oneida School District user violates any of these provisions, his or her account will be terminated and future access could be denied. Certain violations of the Acceptable Use Policy could result in termination of employment with the Oneida School District.

Terms and Conditions:

District Network Acceptable Use Policy

Some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or offensive to some individuals. The District believes that the benefits of access to the Internet far outweigh the risk of being exposed to objectionable material. The burden of appropriate use falls upon the individual user.

The District does use filtering software to block access to inappropriate material on our computer networks. Although this software does block access to many sites, it cannot block all objectionable sites. The filtering system also blocks access to some legitimate sites Internet users may wish to access.

The smooth operation of our network relies on proper conduct of the end users who must adhere to strict guidelines. In general, this requires efficient, ethical and legal utilization of the network and Internet resources. Use of the Network/Internet is a privilege, not a right. The Network/Internet connection is provided for professional and educational purposes only. Unauthorized or inappropriate use will result in a cancellation of this privilege.

1. Use the network in a manner that is responsible, ethical, efficient, and legal. Illegal activities are strictly forbidden.
2. Use of our network for commercial activities is not acceptable. Use for product advertisement or personal political lobbying is also prohibited.
3. Judiciously use resources such as bandwidth, RAM, printers, and paper. Your activities on the network should not disrupt the use of the network by others.
4 Respect others' privacy. Do not access data of another user without their permission. Do not reveal confidential information in a personal online posting, upload or transmission.
5. Respect copyright laws (assume all material is copyrighted unless otherwise stated).
6. Do not remove or exchange any hardware or software components of District computers and do not tamper with installed software or files.

7. Do not install software on District owned computers without permission from the IT Department.
8. Do not use another individual's logon credentials without prior permission from that individual. You take responsibility for actions originating from your account when you allow others to use it. It is your responsibility to change your password when you want to revoke someone's permission to use your account.
9. Notify the District's IT Department of any security problems on our network.
10. Safeguard the data stored on your computer. Make backup copies of important files.
11. All use of social media on the district's network is the sole responsibility of the user to keep secure. The user is responsible for all communications on their accounts.

The District IT Department can monitor your activities on our network.

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions. Use of any information obtained via District's network is at your own risk. The District denies any responsibility for the accuracy or quality of information obtained through its services.

Where it is believed that an employee has failed to comply with this policy, they will face the District's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal.

CURRICULUM
TECHNOLOGY FOUNDATION STANDARDS FOR STUDENTS K-12

The Oneida School District will follow K – 12 state technology standards as well as supporting the technology requirements to support Idaho core standards.

PROFESSIONAL DEVELOPMENT

The Oneida School District will offer opportunity to hone technology skills through professional development opportunities and peer professional development. Other professional development may be provided through district wide initiatives to enhance and support the mission of the district.

TECHNICAL SYSTEMS

It is the goal of the district to continue to expand the IP phone systems, surveillance systems, alarm systems, as well as wireless networks, and a robust network access.

INFRASTRUCTURE

It is the goal of the IT department to provide adequate bandwidth to support classroom instruction. Internet access beyond classroom instructional support may be restricted and limited to ensure the priority of classroom instruction and academic learning support.

HARDWARE

In order to optimize support, the hardware standard below is established by the IT department. Any technology equipment that is purchased outside of this standard or without prior approval of the IT department, must be maintained by the school/teacher and is not permitted to be placed on the district network unless specifically specified by the IT director.

Desktop Computers (supported)
Chromebooks
Chromecasts
ScanSnap Scanners
Printers
TV
Projector
Apple TV
iPads

SOFTWARE

It is the practice of the district to have all software and computer programs approved through the IT department prior to installation and use on district hardware. All software programs must be properly licensed. Annual costs of approved and supported software will be borne by the district. Software that has been approved but is school specific must be maintained and financed through school funding unless specifically specified.

Operating System - Microsoft Windows 10
Approved Hardware Device Drivers
Microsoft Office 2016
Google Chrome
Mozilla Firefox
Java
Adobe Reader
Adobe Flash Player
Adobe Acrobat
Shockwave
VLX Player
WinRAR

REPLACEMENT/UPGRADE STRATEGY

The IT department with the support of the technology committee will develop a three year technology expenditures plan. This will help to guide ongoing support, replacement and upgrade of district technology. While this plan will be closely followed, there will be flexibility to meet unforeseen needs or adjustments to meet the ever changing demands in this field. The labs and teacher stations will be replaced based on performance levels and available funding. Rotation of computers from one lab to another may take place as deemed appropriate by the IT director.

- Infrastructure: It is the goal to provide infrastructure to support the demands of adequate bandwidth.
- File Servers: Rotated every 5 years Updated 6/2016
- Elementary Computers approximately 5-7 years
- Middle school Computers approximately 5-7 years
- High school Computers is approximately 5-6 years
- Telephone system servers 5 years Updated 6/2015
- Routers: Replace every 5 years Updated 6/2015
- Switches : Replace every 5 years Updated 6/2017

TECHNICAL SUPPORT

PROCEDURES: The district has an online work order system which is the sole venue to request technical support and requests for technology repairs. This procedure will make the department more efficient in its response and will help prioritize those requests of immediate need. All work requests are to be sent to helpdesk@malad.us.

The IT department seeks to standardize equipment purchase and support. It is impossible for our small IT department to maintain and support the wide range of technologies. Please check the IT support list prior to any hardware or software purchase.

WEB SITE MAINTENANCE

All website maintenance is to be completed by the District Web Master. All requests should be directed to helpdesk@malad.us

TECHNOLOGY PURCHASING
PURCHASING/COMPATABILITIY

All software, whether stand alone or networked, is reviewed by the District Technology Department before purchase.

Appendix 1

PURCHASING/COMPATABILITIY: TECHNOLOGY PURCHASING FORM

All software, whether stand alone or networked, is reviewed by the District Technology Department before purchase.

Name of person initiating the purchase process:
_____

Name of Building: _____ Date:
_____

Description of hardware or software, which will be purchased (or please attach proposal or quote from
vendor): Detail of location, timeline, and educational uses to which the purchased item will be put:
_____
_____

SCHOOL LEVEL
Principal should review and discuss with faculty

Reviewed and approved by building administrator
_____ _____

Signature Date

DISTRICT LEVEL
Reviewed by District IT Director:
_____ _____
Signature/ Date

☐ **Recommended : _____**

☐ **Not Recommended _____**

Appropriate Use Agreement (Student and Parent)

Every student, regardless of age, must read and sign below:
I have read, understand, and agree to abide by the terms of the Oneida School District's policy regarding District-Provided Access to Electronic Information, Services, and Networks. Should I commit any violation or in any way misuse my access to the District's computer network and/or the Internet, I understand and agree that my access privilege may be revoked and school disciplinary action may be taken against me.

User's Name (Print): _____ Home Phone:_____
User's Signature: _____ Date: _____
Address:_____

If I am signing this policy when I am under 18, I understand that when I turn 18, this policy will continue to be in full force and effect and agree to abide by this policy.
Parent or Legal Guardian. (If applicant is under 18 years of age, a parent/legal guardian must also read and sign this agreement.) As the parent or legal guardian of the above-named student, I have read, understand, and agree that my child shall comply with the terms of the District's policy regarding District-Provided Access to Electronic Information, Services, and Networks for the student's access to the District's computer network and/or the Internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the school to restrict access to all offensive and controversial materials and understand my child's responsibility for abiding by the policy. I am, therefore, signing this Agreement and agree to indemnify and hold harmless the District, the Trustees, Administrators, teachers, and other staff against all claims, damages, losses, and costs, of whatever kind, that may result from my child's use of or access to such networks or his/her violation of the District's policy. Further, I accept full responsibility for supervision of my child's use of his/her access account if and when such access is not in the school setting. I hereby give my child permission to use the building-approved account to access the District's computer network and the Internet.
Parent/Legal Guardian (Print):
_____
Signature:
_____
Home Phone: _____ Address:
_____
Date: _____
This Agreement is valid for the _____ school year only.

Oneida School District
Software Programs
2019-2020

District

PowerSchool – $15,000 (Paid by district)
PowerSchool Learning- $7,000
PowerSchool Performance Matters - $7,000
PowerSchool Registration - $7,000
Swift K Reach – $1,890 (Paid by district)
Frameworks – $3300 (Paid by district)
Blue Bear – $2823 (Paid by district)
Instant Payments – Free
Edmentum – Free (Paid by SDE)
Imagine Math – Free (Paid by SDE)
Discovery Education - $28,000 (Paid for up to 2025)
i-Ready – $32,000
EduTyping - $1,800 (Paid for up to 2021)
IStation – Free (Paid by SDE- K-3)
iTrack - $1,105 (Paid with Special Education funds)
Microsoft IT Academy – Free (Paid by SDE)
Google Apps for Education – Free
OETC Microsoft licenses - $3,831 (Paid by Technology Account)
SmoothWall (Web Filter/Firewall) - $5,000 (Paid by Technology Account)

MES

Follett – $649

MMS

MobyMax Paid for through 2022
IXL Paid for through 2020

MHS

Follet - $1,100

Malad High School Student/Parent Agreement For Chromebook Use

– I will take good care of my assigned Chromebook.
– I will never leave my Chromebook unattended.
– I will never loan out my Chromebook to other individuals.
– I will know where my Chromebook is at all times.
– I will charge my Chromebook's battery daily.
– I will keep food and beverages away from my Chromebook.
– I will not disassemble any part of my Chromebook or attempt any repairs.
– I will protect my Chromebook by transporting it in the case provided.
– I will use my Chromebook in ways that are appropriate and educational.
– I will keep personal information about myself or others off the Chromebook.
– I understand a school district employee can take my Chromebook away at anytime. I will report any damage to my Chromebook or loss of my Chromebook to the school district immediately.
– I will not allow any outside individual or company to attempt any repair of my device.
– I will keep all passwords private and not share them with other individuals.
– I will not place decorations (such as stickers, markers, etc.) on the Chromebook.
– I will not deface the serial number, Chromebook asset number, or any identifying sticker on any Chromebook.
– I understand that my Chromebook is subject to inspection at any time without notice and remains the property of the Oneida School District.
– I will be responsible for all damage or loss caused by neglect or abuse.
– I agree to return the Chromebook, charger, and case in good working condition.
– I realize that if I break or damage my Chromebook in any manner or at any time including while at school, I am responsible to pay the replacement cost or the cost to repair the device.

I understand and agree to the stipulations set forth in the above document.

Student Name (please print):

_____

Student Signature:

_____

Parent Signature:

_____

Date: _____

1:1 Chromebook Project

Insurance Plan

I, _____, elect to participate in the 1:1 Chromebook Project Insurance Plan for my student, _____.

☐ $50.00 Annual Premium – Insurance starts after the Annual Premium has been paid to Malad High School.

As a participant in this insurance program I will receive the following benefits:

1. Damage Coverage: If the Chromebook is damaged and/or the Chromebook Power Cord is lost or damaged, I will pay 50% of the cost of repairs or a $75.00 deductible, whichever is less.

2. Total Replacement: If the Chromebook needs to be replaced, I will pay a $100.00 deductible.

Malad High School administration reserves the right to quote the costs of repairs and replacements. All deductibles must be paid before the repaired or replaced Chromebook and/or Power Cord are provided to the student.

_____ _____

Parent/Guardian Signature Date

YEAR	DEVICES	BUDGET
2019-2020	MHS Chromebooks-200 10 Teachers Computers Server Maintenance and Repairs Touch Screen Chromebooks or iPads Projectors/TV's – 5 Laptops Scanners	$40,000 $6,500 $1,400 $5,000 $24,000 – $50,000 $5,000 $15,000 $4,000
2020-2021	MHS Chromebooks-200 10 Teachers Computers Server Maintenance and Repairs Projectors/TV's – 10 Laptops Scanners	$40,000 $6,500 $1,400 $5,000 $10,000 $15,000 $4,000
2021-2022	MHS Chromebooks-200 10 Teachers Computers Server Maintenance and Repairs Projectors/TV's – 10 Laptops Scanners	$40,000 $6,500 $1,400 $5,000 $10,000 $15,000 $4,000

PERSONNEL

Employee Use of Electronic Communications Devices

Employee use of electronic communication and entertainment devices may interfere with or disrupt the educational process as well as distract personnel from their job responsibilities. Personnel are required to limit their use of electronic communication and entertainment devices to emergencies or during authorized breaks. Such devices are prohibited from being used during instructional time unless the specific use is consistent with the lesson plan being presented. Violation of this policy may result in disciplinary action up to and including termination.

PROFESSIONAL COMMUNICATIONS

All employees are assigned an e-mail account for work-related correspondence. When communicating with students, or parents regarding a school related issue, employees shall only use their school issued email account or other administration approved email system.

COMMUNICATIONS WITH STUDENTS

The board recognized that there are occasions when a person in a district approved position (e.g. employee, coach, volunteer, or other persons in official or approved district positions) may have a legitimate need to communicate with a student outside of school hours. Any communication between a person in a district approved position and student via telecommunications, text messages, emails, and/or any other medium must be professional in content and tone. Employees should not make any statements or forward information which could reasonably be perceived to be:

1. Sexually suggestive, obscene, vulgar, or inappropriate in content;
2. Developing an inappropriate relationship with a student; (including sending/receiving an inordinate number of communications; communicating at an inappropriate time of day/night);
3. Harmful to a student;
4. Disruptive of the educational process;
5. In violation of federal or state laws, or district policies; or in violation of FERPA and other confidentiality requirements.

Any communications with students may be subject to review by the district if the material violates district policy and comes to the attention of the district. In the event an employee receives any communication from a student which is inappropriate in nature, the employee has an obligation to report such communication to the building administrator or designee.

SOCIAL NETWORKING

The board recognized that employees may engage in social networking, whether through sites such as Facebook, LinkedIn, maintain blogs, or participate in such media as email groups, YouTube, or Twitter, or have a public presence on the Internet by similar means. While such activities are not part of the employee's work responsibilities, employees may communicate with and/or be identified with patrons, parents and students of the district.

Employees are expected to comply with the following guidelines:

1. An employee shall not engage in social media during contract time.
2. Social media interactions cannot be one on one between employees and students.
3. An employee must recognize that statements or innuendo publicly displayed on the Internet may have negative ramifications on that individual's position as a role model for students of the district. Statements deemed damaging towards a school, the district, or a classroom will compromise an employee's ability to fulfill their responsibilities, thus resulting in corrective action up to termination.
4. An employee should always present himself/herself in a professional manner and exercise good judgment relative to any information he/she posts or any sites linked to his/her social network page or blog.

5. Information posted by an employee must comply with the state and federal laws and district policies relative to confidentiality. If the employee posts information that evidences that the employee has engaged in conduct in violation of applicable federal and state law, or district policies, the district may turn the incident over to the Professional Standards Commission for an investigation and/or take disciplinary action, up to and including termination.

DEFINITION

"Electronic communication and entertainment devices" shall include, but not be limited to, personal cell phones, iPods, MP3 players, and other similar devices or media players, without regard to the commercial name or manufacturer of the device, whether handheld, car models, laptop or other computer usage, or combinations of any of the above

STUDENTS

District-Provided Access to Electronic Information, Services, and Networks

General

Internet access and interconnected computer systems are available to the District's students and faculty. Electronic networks, including the Internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

In order for the District to be able to continue to make its computer network and Internet access available, all users, including students, must take responsibility for appropriate and lawful use of this access. Students utilizing school-provided Internet access are responsible for good behavior on-line. The same general rules for behavior apply to students' use of District-provided computer systems. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the District's teachers and other staff will make reasonable efforts to supervise use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Curriculum

In accordance with this policy and the Board's philosophy to ensure the safety of all students, the District shall provide an appropriate planned instructional component for internet safety which shall be integrated into the District's regular instructional program. The purpose of the program is to increase students' knowledge of safe practices for internet use.

The use of the District's electronic networks shall be consistent with the curriculum adopted by the District, as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and shall comply with the selection criteria for instructional materials and library-media center materials. Staff members may, consistent with the District's educational goals, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Responsible Uses

1. Educational Purposes Only. All use of the District's electronic network must be (1) in support of education and/or research, and in furtherance of the District's stated educational goals; or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to monitor, inspect, copy, review and store, at any time and without prior notice, any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage.

2. Unacceptable Uses of Network. The following are considered examples of unacceptable uses and constitute a violation of this policy. Additional unacceptable uses can occur other than those specifically listed or enumerated herein:

A. Uses that violate the law or encourage others to violate the law, including but not limited to transmitting offensive or harassing messages; offering for sale or use any substance the possession or use of which is prohibited by the District's student

discipline policy, local, state, or federal law; viewing, transmitting or downloading pornographic materials or materials that encourage others to violate local, state, or federal law; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials.

B. Uses that cause harm to others or damage to their property, person or reputation, including but not limited to engaging in defamation (harming another's reputation by lies); employing another's or some other user identifier that misleads message recipients into believing that someone other than you is communicating, or otherwise using his/her access to the network or the Internet; uploading a worm, virus, other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or other information.

C. Uses amounting to harassment, sexual harassment, bullying or cyber-bullying defined as using a computer, computer system, or computer network to convey a message in any format (audio or video, text, graphics photographic, or any combination thereof) that is intended to harm another individual.

D. Uses that jeopardize the security of student access and of the computer network or other networks on the Internet.

E. Sending, receiving, viewing or downloading obscene materials, materials harmful to minors and materials that depict the sexual exploitation of minors.

Internet Safety

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The school will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or other material that is inappropriate for minors. The Superintendent or designee shall enforce the use of such filtering devices. The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that:

- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to 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;
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. The term "harmful to minors" is defined in Section 18-1514(6), Idaho Code as meaningone or both of the following:
- The quality of any material or of any performance of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it:
- Appeals to the prurient interest of minors as judged by the average person, applying contemporary community standards; and
- Depicts or describes representations or descriptions of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse which are patently offensive to prevailing standards in the adult community with respect to what is suitable material for minors and includes, but is not limited to, patently offensive representations or descriptions of:

Intimate sexual acts, normal or perverted, actual or simulated; or Masturbation, excretory functions or lewd exhibits of the genitals or genital area. Nothing herein contained is intended to include or proscribe any matter which, when considered as a whole, and in context in which it is used, possesses serious literary, artistic, political or scientific value for minors, according to prevailing standards in the adult community, with respect to what is suitable for minors.

• The quality of any material or of any performance, or of any description or representation, in whatever form, which, as a whole, has the dominant effect of substantially arousing sexual desires in persons under the age of eighteen (18) years.

Internet Filtering

Filtering should be only one of a number of techniques used to manage student's access to the Internet and encourage acceptable usage. It is not viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors. Anything that falls under at least one of the categories below shall be blocked/filtered. This list will be updated/modified as required.

- Nudity/ pornography – prevailing U.S. standards for nudity, provocative semi-nudity, sites which contain pornography or links to pornographic sites
- Sexuality – sites which contain material of a mature level, images or descriptions of sexual aids, descriptions of sexual acts or techniques, sites which contain inappropriate personal ads
- Violence – sites which promote violence, images or description of graphically violent acts, graphic autopsy or crime-scene images
- Crime – information of performing criminal acts (e.g., drug or bomb making, computer hacking), illegal file archives (e.g., software piracy)
- Drug Use – sites which promote the use of illegal drugs, material advocating the use of illegal drugs (e.g. marijuana, LSD) or abuse of any drug. Exception: material with valid-educational use
- Tastelessness – images or descriptions of excretory acts (e.g., vomiting, urinating), graphic medical images outside of a medical context
- Language/Profanity – passages/words too coarse to be softened by the word filter, profanity within images/sounds/multimedia files, adult humor
- Discrimination/Intolerance – Material advocating discrimination (e.g., racialor religious intolerance), sites which promote intolerance, hate or discrimination
- Interactive Mail/Chat – sites which contain or allow inappropriate email correspondence, sites which contain or allow inappropriate chat areas
- Inappropriate Banners – advertisements containing inappropriate images or words
- Gambling – sites which allow or promote online gambling
- Weapons – sites which promote illegal weapons, sites which promote the use of illegal weapons
- Body Modification – sites containing content on tattooing, branding, cutting, etc.
- Judgment Calls – whether a page is likely to have more questionable material in the future (e.g., sites under construction whose names indicate questionable material)

Filtering should also be used in conjunction with:

- Educating students to be "Net-smart;"
- Using recognized Internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;
- Using "Acceptable Use Agreements;"
- Using behavior management practices for which Internet access privileges can be earned or lost; and
- Appropriate supervision, either in person and/or electronically.

The system administrator and/or building principal shall monitor student Internet access. Upon request and under the supervision of the system administrator, an Internet site or sites may be white-listed for the purpose of bona fide research or other educational projects being conducted in the school. Review of filtering technology and software shall be done on a periodic basis and is the responsibility of the Internet Safety Coordinator. It shall be the responsibility of the Internet Safety Coordinator to bring to the Board any suggested modification of the filtering system and to address and assure that the filtering system meets the standards of Idaho Code 18-1514 and any other applicable provisions of Chapter 15, Title 18, Idaho Code.

Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and social security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

Internet Access Conduct Agreements

Each student and his/her parent(s)/legal guardian(s) will be required to sign and return to the school at the beginning of each school year the Internet Access Conduct Agreement prior to having access to the District's computer system and/or Internet Service.

Warranties/Indemnification

The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. The District will not be responsible for any unauthorized charges or fees resulting from access to the Internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event of the school's initiating an investigation of a user's use of his/her access to its computer network and the Internet.

Violations

If any user violates this policy, the student's access to the school's internet system and computers will be denied and he/she may be subject to additional disciplinary action. The system administrator and/or the building principal will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with his/her/their decision being final. Actions which violate local, state or federal law may be referred to the local law enforcement agency. If the actions of the individual are also in violation of other District discipline policies, said student shall be subject to additional possible disciplinary action based upon these policies.
Internet Safety Coordinator

The Superintendent shall serve, or appoint someone to serve, as “Internet Safety Coordinator” with responsibility and authority for ensuring compliance with the requirements of federal law, state law and this policy. The Internet Safety Coordinator shall develop and maintain administrative procedures to enforce the provisions of this policy and coordinate with the appropriate District personnel regarding the internet safety component of the District’s curriculum. The Internet Safety Coordinator shall handle any complaints about the enforcement of this policy. The Internet Safety Coordinator shall maintain documentation evidencing that instruction by school personnel on internet safety is occurring District wide.

Public Notification

The Internet Safety Coordinator shall inform the public via the main District webpage of the District’s procedures regarding enforcement of this policy and make them available for review at the District office.

STUDENTS

District Provided Mobile Computing Devices

Oneida School District is committed to providing a safe, rigorous, and engaging learning environment that prepares all students to be career and college ready. Accessing and using technological resources is one of the cornerstones of a 21st Century education. This document describes the rules for acceptable use of District-issued mobile computing devices on and off District premises. Using these resources responsibly will promote educational excellence by facilitating resource sharing, fostering creativity, and promoting communication in a safe, secure environment for all users.

Distributing Mobile Computing Devices

Before they are issued a mobile computing device, each student must submit an executed Agreement for Mobile Computing Device Use indicating they understand and agree with the district Responsible Use Policy 3270. Each form must be signed by the student and by their parent or guardian.
The District may provide parent orientations on the mobile computing device program. A student's parents or guardians are encouraged to attend an orientation before the student takes a device home with them. The student may choose to pay an insurance fee of $50 before they may take the device home.
Parents or guardians of students may use the school-issued device, and their involvement in student learning through technology is strongly encouraged. However, use of school-issued technology outside of this purpose, such as for personal gain or activities unrelated to student learning, is prohibited. Both parent and student use of the District's device, network, and software may be subject to a public records request depending upon the content of the document or communication, including email.
At the end of the school year, the school will collect all devices from students. At the school's discretion, students may be issued devices to support summer school programs.
The Superintendent shall establish procedures for the maintenance of records regarding the devices, including tracking device inventory and which device is issued to which student.

Care and Safety

Students are responsible for the general care of the device they have been issued by the District and are expected to observe the following precautions:

1. No food or drink is allowed next to a device while it is in use;
2. Insert and remove cords, cables, and removable storage devices carefully;
3. Shut down the device when not in use to conserve battery life;
4. Stickers, drawings, or permanent markers may not be used on the device;
5. Do not vandalize the devices or any other school property;
6. Devices must never be left in any unsupervised area.
7. Students are responsible for keeping their device's battery charged for school each day;
8. Do not place anything near the device that could put pressure on the screen;
9. Clean the screen with a soft, dry cloth or anti-static cloth;
10. Devices should not be stored in a student's vehicle, or anyplace else subject to extreme temperatures.
11. Never loan out their device to other individuals.
12. Do not disassemble any part of their device or attempt any repairs.

13. Students will not deface the serial number, asset number, or any identifying tags on the device.
14. Protect the device by transporting it in the case provided.
15. Never allow any outside individual or company to attempt any repair of the device.

The Superintendent will designate an individual or office at the school level where the devices must be taken if they break or fail to work properly.

Use at School

Devices are intended for use at school each day. Students are responsible for bringing their device to all classes, unless specifically advised not to do so by their teacher. Devices must be brought to school each day in a fully charged condition. Repeat failures to comply with these requirements will result in disciplinary action. If students leave their device at home, they may phone parent/guardian to bring it to school. Sound must be muted or headsets must be used at all times unless the teacher directs otherwise.

Students may use printers in classrooms, the library, and computer labs with teachers' permission during class or breaks. All printing should be limited to educational purposes.

Personalizing Mobile Computing Devices

While at no time does the device become the personal property of students or staff; students may place individualized items on the device, which are limited to music, pictures, and other items that do not hinder the network or device functionality. Students may be permitted to select their own screen savers and backgrounds provided they are appropriate. Screensavers, backgrounds, or other pictures containing guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, gang related symbols or pictures, the student's password or other items deemed inappropriate by the administration will result in disciplinary actions.

Students may not add options or upgrades to the device, change the operating system, or add unauthorized software or safety controls.

Should students or parents/guardians place personalized items on the device, such items may be accessed or viewed by District staff at any time, for any reason, including randomly selected device reviews. No content placed on District provided devices is privileged or confidential.

Managing Files

Once details are known about the availability of file space that is shared or is backed up automatically, the Superintendent will set a procedure for where students and teachers should save important documents.

Students should also back up their work frequently using removable file storage or by e-mailing important document to themselves. It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work.

Software

The software originally installed by the District must remain on the device in usable condition and

be easily accessible at all times. From time to time the school may add or update software applications. The licenses for this software sometimes require that the software be deleted from devices at the completion of a course.
Periodic reviews of devices will be made to ensure that students have deleted software that is no longer required in class and that the school has not exceeded its licenses.
Some devices will be equipped with anti-virus protection software which will be upgraded regularly. It is the responsibility of individual students to be aware of additional software programs and files loaded onto their device which are required for classes or school activities.
Students wishing to add additional software onto a device must first obtain the permission of the school's technology department. Any additional software must be appropriate for the school environment and comply with the Responsible Use Policy. Violent games and device images containing obscene or pornographic material are banned. The technology department shall determine whether a game is violent, and the student may appeal this decision to the principal. Each student is responsible for ensuring that only licensed software is loaded onto his or her device.

Inspection and Filtering

Filtering software will be used to prevent access to material considered inappropriate or harmful to minors.
Students may be selected at random or for cause to provide their device for inspection. If technical difficulties occur or unauthorized software or any other violation of District policy is discovered, all files and the hard drive may be reformatted. Only authorized software will be installed. The District does not accept responsibility for the loss of any software or other materials deleted due to a reformat and reimage.
Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of law.

Remote Access of Devices

Devices may be equipped with the ability to be accessed remotely in the case of technical problems requiring remote assistance, missing or stolen devices, or other for any other appropriate District purpose. A student does not need to be asked for permission prior to remote software maintenance.

Acceptable Use

Access to the devices is a privilege and not a right. Each employee, student, and parent will be required to follow the District Responsible Use Policy #3270. Violation of these policies, whether by the student or another party, while the device is in student custody may result in disciplinary action for the student, possible revocation of device privileges, and/or contacting law enforcement authorities.

Protecting and Storing Devices

Students are expected to password protect their devices and shall keep their password confidential. When students are not using their devices, the devices should be stored in their lockers. Students are encouraged to take their devices home every day after school.

Under no circumstances should devices be left in unsupervised areas. Unsupervised areas include the school grounds, the cafeteria, computer lab, locker rooms, library, unlocked classrooms, dressing rooms, and hallways. Unsupervised devices will be confiscated by staff and taken to the building principal's office. Disciplinary action may be taken for leaving a device in an unsupervised location.

Repair of Devices

Students are to report all device problems to helpdesk@malad.us or a building administrator. The Superintendent will issue a document clarifying student or parent responsibility for lost and damaged devices when the details of the District's insurance policy are known.