NORTHWEST TECHNOLOGY CENTER BOARD OF EDUCATION POLICY	*Technology* Adopted: June 5, 2017

INTERNET AND TECHNOLOGY SAFETY PURSUANT TO THE CHILDREN'S INTERNET PROTECTION ACT

It is the policy of the technology center to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic or digital communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 U.S.C. §254(h)].

Definition

Key terms as defined in the Children's Internet Protection Act:

Access to Inappropriate Material - To the extent practical, technology protection measures (or "Internet Filters") shall be used to block or filter Internet (or other forms of electronic or digital communications) access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

Any individual who uses the technology center's resources to access the Internet or engage in any electronic or digital communication is required to participate in the technology center's education efforts (undertaken pursuant to the Children's Internet Protection Act) and comply with the district's acceptable use policy.

Supervision and Monitoring

All employees are responsible for supervising and monitoring minor student's use of the Internet in accordance with the technology center's policies and the Children's Internet Protection Act. The technology center's IT director shall establish and implement procedures regarding technology protection measures. No individual will be permitted to use the school's technology resources in a manner inconsistent with the technology center's policies.

Personal Safety

Employees and students shall not use the school's technology resources in any manner that jeopardizes personal safety. Students and employees must follow the technology center's

policies, including the acceptable use policy which details the technology center's safe use standards.

ACCEPTABLE USE OF INTERNET AND ELECTRONIC AND DIGITAL COMMUNICATIONS DEVICES

The forms of electronic and digital communications change rapidly. This policy addresses common existing forms of electronic and digital communication (email, texting, blogging, tweeting, posting, etc.) but is intended to cover any new form of electronic or digital communication which utilizes a computer, phone or other digital or electronic device.

As a part of the resources available to students and employees, the technology center provides Internet access at each campus and at its administrative offices. The technology center intends for this resource to be used for educational purposes and not to be used for conduct which is harmful. This policy outlines the technology center's expectations regarding Internet access. The ability to access the Internet while on technology center property is a privilege and not a right. Access cannot be granted until an individual has completed an "Internet Access Agreement" and access may be revoked at any time.

Any individual using technology center resources to engage in electronic or digital communications has no expectation of privacy. Further, employees and students must be cognizant of the fact that electronic or digital communications which occur on private equipment are often permanently available and may be available to school administrators.

Employees and students are expected to use good judgment in all their electronic or digital communications - whether such activities occur on or off campus or whether the activity uses personal or school technology. Any electronic or digital communication which can be considered inappropriate, harassing, intimidating, threatening or bullying to an employee or student of the technology center - regardless of whether the activity uses technology center equipment or occurs during school/work hours - is strictly forbidden. Employees and students face the possibility of penalties, including student suspension or dismissal and employee termination, for failing to abide by technology center policies when accessing and using electronic or digital communications.

The Internet provides users the ability to quickly access information on any topic - even topics which are considered harmful to minors. The technology center's IT department has attempted to filter this access in order to protect students from harmful content. In the event inappropriate material is inadvertently accessed, students should promptly report the site to their instructor so that other students can be protected. No individual is permitted to circumvent the technology center's privacy settings by accessing blocked content through alternate methods. In the event an employee needs access to blocked content, he/she should make arrangements through the campus director or IT director.

Although the technology center's IT department has taken appropriate steps to block offensive material, users may unwittingly encounter offensive material. All users of the technology center's electronic resources are required to exercise personal responsibility for the material they access, send or display, and must not engage in electronic conduct which is prohibited by law or policy. If a student inadvertently accesses or receives offensive material, he/she should report

the communication to the assigned instructor. If an employee accesses or receives offensive material, he/she should report the communication to the campus director or IT director. No individual is permitted to access, view or distribute materials which are inappropriate or create a hostile environment.

Internet Access - Terms and Conditions.

Acceptable Use - Students. Students agree to access material in furtherance of educational goals or for personal leisure and recreational use which does not otherwise violate this policy. No student may make an electronic or digital communication which disrupts the education environment - even if that communication is made outside of school or on personal equipment. Types of electronic or digital communications which can disrupt the education environment include, but are not limited to:

- Sexting
- Harassing, intimidating, threatening or bullying posts, tweets, blogs, images, texts, etc.
- Distributing pictures, recordings or information which is harmful or embarrassing

Students who engage in electronic or digital communications which disrupt the education environment are subject to disciplinary action, including suspension or dismissal from school. Depending on the nature of the electronic or digital communication, students may also be subject to civil and criminal penalties.

Acceptable Use - Employees. Employees agree to access material in furtherance of educational goals, including research and professional development. Employees are also permitted to judiciously use the technology center's electronic resources for limited personal use, provided that the use is of no cost to the technology center, does not preempt business activity, impede productivity, or otherwise interfere with work responsibilities. Electronic or digital communications made using technology center owned equipment must be professional in nature and cannot be used for the exercise of the employee's free speech rights.

Any electronic or digital communication in which the employee can be identified as an employee of the technology center – regardless of whether the communication is made with technology center owned equipment or during work hours - must be a professional communication. Accordingly, if the individual is identifiable as a technology center employee, electronic or digital communications must not contain sexual, harassing, discriminatory or immoral content. Further, the communication cannot promote the use of tobacco, drugs, alcohol or be otherwise inconsistent with the technology center's objectives.

Employees are required to maintain appropriate electronic boundaries with students. Such boundaries require that employees refrain from engaging in electronic or digital communications which show an undue interest in select student(s), are of a personal nature, model inappropriate conduct, or are otherwise inconsistent with the technology center's mission and goals. In order to maintain appropriate boundaries, the technology center encourages employees to:

- Send group texts or emails
- Use separate personal and school electronic accounts
- Obtain written parental permission prior to posting pictures of minors
- Respect individual privacy, including privacy rights granted by FERPA

Employees are expressly forbidden from using electronic or digital communication in a manner inconsistent with their position as a role model for students. Any employee who engages in inappropriate electronic or digital communication with students is acting outside the scope of his/her employment with the technology center.

Prohibited Use. Users specifically agree that they will not use the Internet to access material which is: threatening, indecent, lewd, obscene, or protected by trade secret. Users further agree that they will not use the technology center's electronic resources for commercial activity, charitable endeavors (without prior administrative approval), product advertisement or political lobbying.

Parental Consent. Parents of minor students must review this policy with their student and sign the consent form prior to a minor student being granted Internet access.

Privilege of Use. The technology center's electronic resources, including Internet access, is a privilege which can be revoked at any time for misuse. Prior to receiving Internet access, all users will be required to successfully complete an Internet training program administered by the technology center.

Internet Etiquette. All users are required to comply with generally accepted standards for electronic or digital communications, including:

a. Appropriate Language. Users must refrain from the use of abusive, discriminatory, vulgar, lewd or profane language in their electronic or digital communications.

b. Content. Users must refrain from the use of hostile, threatening, discriminatory, intimidating, or bullying content in their electronic or digital communications.

c. Safety. Minor students must not include personal contact information (name, address, phone number, address, banking numbers, etc.) in their electronic or digital communications. Minor students must never agree to meet with someone they met online and must report any electronic or digital communication which makes them uncomfortable to their teacher.

d. Privacy. Users understand that the technology center has access to and can read all electronic or digital communications created and received with technology center resources. Users agree that they will not use technology center resources to create or receive any electronic or digital communications which they want to be private.

e. System Resources. Users agree to use the technology center's electronic resources carefully so as not to damage them or impede others' use of the technology center's resources. Users will not:

- install any hardware, software, program or app without approval from the IT department
- download large files during peak use hours
- disable security features
- create or run a program known or intended to be malicious
- stream music or video for personal entertainment

f. Intellectual Property and Copyrights. Users will respect others' works by giving proper credit and not plagiarizing, even if using websites designed for

educational and classroom purposes (*See* www.copyright.gov/fls/fl102.html) Users agree to ask their instructor for assistance in citing sources as needed.

Limitation of Liability. The technology center makes no warranties of any kind, whether express or implied, for the services provided and is not responsible for any damages arising from use of the technology center's technology resources. The technology center is not responsible for the information obtained from the use of its electronic resources and is not responsible for any charges a user may incur while using its electronic resources.

Security. If a user notices a potential security problem, he/she should notify the IT director immediately but should not demonstrate the problem to others or attempt to identify potential security problems. Users are responsible for their individual account and should not allow others to use their account. Users should not share their access code or password with others. If a user believes his/her account has been compromised, he/she must notify the IT director immediately. Any attempt to log on to the technology center's electronic resources as another user or administrator, or to access restricted material, may result in the loss of access for the remainder of the school year or other disciplinary measures.

Vandalism. No user may harm or attempt to harm any of the technology center's electronic resources. This includes, but is not limited to, uploading or creating a virus or taking any action to disrupt, crash, disable, damage, or destroy any part of the technology center's electronic resources. Further, no user may use the technology center's electronic resources to hack vandalize another computer or system.

Inappropriate Material. Access to information shall not be restricted or denied solely because of the political, religious or philosophical content of the material. Access will be denied for material which is:

a. Obscene to minors, meaning (i) material which, taken as a whole, lacks serious literary, artistic, political or scientific value for minors and, (ii) when an average person, applying contemporary community standards, would find that the written material, taken as a whole, appeals to an obsessive interest in sex by minors.

b. Libelous, meaning a false and unprivileged statement about a specific individual which tends to harm the individual's reputation.

c. Vulgar, lewd or indecent, meaning material which, taken as a whole, an average person would deem improper for access by or distribution to minors because of sexual connotations or profane language.

d. Display or promotion of unlawful products or services, meaning material which advertises or advocates the use of products or services prohibited by law from being sold or provided to minors.

e. Group defamation or hate literature, meaning material which disparages a group or a member of a group on the basis of race, color, sex, pregnancy, gender, gender expression or identity, national origin, religion, disability, veteran status, sexual orientation, age or genetic information or advocates illegal conduct or violence or discrimination toward any particular group of people. This includes racial and religious epithets, "slurs," insults and abuse.

f. Disruptive school operations, meaning material which, on the basis of past experience or based upon specific instances of actual or threatened disruptions relating to the information or material in question, is likely to cause a material

and substantial disruption of the proper and orderly operation of school activities or school discipline.

Application and Enforceability. The terms and conditions set forth in this policy shall be deemed to be incorporated in their entirety in the Internet Access Agreement executed by each user. By executing the Internet Access Agreement, the user agrees to abide by the terms and conditions contained in this policy. The user acknowledges that any violation of this policy may result in access privileges being revoked and disciplinary action being taken. For students, this means any action permitted by the technology center's policy on student behavior. For employees, this means any action permitted by law, including termination of employment.

Education of Students Regarding Appropriate On-Line Behavior. In compliance with the Protecting Children in the 21st Century Act, Section 254(h)(5), the technology center provides education to minors about the appropriate use of the technology center's electronic resources, including interacting with others on social networking and chat sites, and cyber bullying. As a part of that education, guidelines on cyber bullying and internet safety for students are attached to this policy.

Cyber Bullying and Internet Safety Fact Sheet

People can be bullied in lots of ways, including through cyber bullying. Cyber bullying is when someone sends or posts things (words, pictures, recordings) that are mean, embarrassing or make people feel scared, embarrassed or uncomfortable. Even if they don't do this at school sometimes cyber bullying makes things at school hard. No student is allowed to disrupt school through cyber bullying.

Cyber bullies work in lots of ways, but here's some of their most common:

- Send or post mean messages
- Make up websites or accounts with stories, cartoons, pictures or "jokes" that are mean to others
- Take embarrassing pictures or recordings (without asking first)
- Send or post stuff to embarrass others
- Hack into other people's accounts or read their stuff
- Hack into other people's accounts and send or post their private stuff
- Pretend to be somebody else to get someone to give them private info
- Send threats

If you're a cyber bully knock it off! Ask your principal/counselor how you can make things right.

If someone is cyber bullying you, there's something you can do about it:

- Don't respond to and don't ignore a cyber bully. Instead, tell an adult you trust. If cyber bullying follows you to school, tell your teacher or counselor.
- Even if what the bully does is embarrassing, don't delete it. Instead, get a copy so you can prove what happened.
- Have an adult help you contact a company representative (cell phone company, Yahoo, Facebook, Twitter, etc.) about blocking or removing the bad stuff.

You can't always stop people from being mean, but there are ways to help yourself:

- Don't give out your personal info in electronic or digital communications
- Don't tell anyone but your parents what your login name, password or PIN number is
- Don't post or send embarrassing pics or recordings (even on your own sites) - bullies love to copy your stuff

Suggestions for Parents:

- Help your child understand how permanent electronic or digital communications are
- Talk to your child about understanding, preventing and responding to cyber bullying
- Contact your student's school for help if you suspect your child is being cyber bullied – or if you suspect your child is engaging in cyber bullying

PROHIBITED USE OF DISTRICT ISSUED TECHNOLOGY EQUIPMENT

The technology center may issue a wireless device to the employee such as a cell phone, IPad, or laptop. Employees who are issued these devices must carefully adhere to all other technology policies.

For business and tax reasons the personal use of such equipment is not permitted and, as a result, any personal use should be limited to emergency circumstances. Any employee who utilizes a school wireless device for personal reasons must promptly notify his/her supervisor in writing, and all usage records are subject to audit for compliance with this policy. Employees who violate these requirements are subject to disciplinary action, including removal of the equipment or termination.

Any employee who is issued a technology center owned wireless device must protect the device from loss, damage, or theft. If the device is lost, the employee must promptly report the loss to his/her supervisor. If the device is stolen, the employee must immediately file a police report and notify his/her supervisor.

Employees must return all wireless devices, in good condition, upon request of the technology center or upon separation from employment, whichever is sooner.

PERSONAL WIRELESS DEVICES

The technology center requires that all individuals devote their full attention to education while at school or during education activities. Accordingly, the technology center expects both employees and students to limit their use of personal wireless devices at school. Wireless devices include, but are not limited to, cell phones, laptops, cameras, GPS systems, any type of device capable of intercepting or recording a conversation, any type of device capable of providing visual surveillance or images, recorders, Google Glass, etc.

Google Glass and similar technology is prohibited on campus by all individuals at all times. Regardless of the type of technology used, no individual may make any type of surreptitious recording of others on district property. Additionally, no person may use any type of technology to remotely monitor, listen to, or view actions occurring at school or school activities.

Personal wireless devices not otherwise prohibited shall be turned off and out-of-sight in locations such as restrooms, locker rooms, changing rooms, etc. ("private areas"). The use of any audio/visual recording and camera features are strictly prohibited in private areas. Students who observe a violation of this provision shall immediately report this conduct to a teacher, administrator or campus director. Employees who observe a violation of this provision shall immediately report this conduct to a supervisor or the campus director.

Students

Students who violate this policy will have their personal wireless device confiscated until after a parent conference, and may lose the privileges of possessing such a device for the remainder of the school year. Students are also subject to other disciplinary action.

Students may not use any personal wireless device to:

- send or receive answers to test questions;
- record conversations or events during the school day, on technology center property or at technology center activities;
- threaten, harass, intimidate, or bully;
- take, possess, or distribute obscene or pornographic images or photos;
- engage in lewd communications;
- violate technology center policies, handbook provisions, or regulations.

Employees

Personal wireless devices may only be used during work time if the use of the device furthers the employee's performance of his/her professional responsibilities. No employee may use work time to engage in any personal electronic or digital communication, Internet activity, gaming,

etc. Employees will make reasonable efforts to use technology center resources rather than personal wireless devices for electronic or digital communications with other employees, parents, and students.

Employees are not permitted to text or otherwise use a personal wireless device while operating a technology center vehicle.

Personal wireless devices may not be used to photograph or record conversations or events outside private areas without first obtaining consent to record from all parties. In the case of students, permission from the campus director must be obtained. Administrative approval for recordings of students will take into consideration whether prior approval has been granted from parents/guardians of minors and whether the recording would identify a specific category of students such as special education students.

Personal wireless devices may only be shared with students for emergency use.

No employee may use a personal wireless device to engage in conduct which is illegal or which could be construed as inappropriate conduct with a student or students. In the event an employee receives an inappropriate electronic or digital communication from a student or parent, the communication must be promptly reported to the employee's supervisor.

The technology center fully acknowledges that personal wireless communications devices are the personal property of the employee. Unless an administrator has reasonable suspicion that an employee's personal equipment contains prohibited content, an administrator may not inspect an employee's personal equipment without the employee's express consent.

Warning: Possessing, taking, disseminating, transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images, photographs, or communications, whether by electronic data transfer or otherwise (commonly called texting, sexting, emailing, and other modes of electronic or digital communication) may constitute a CRIME under state and/or federal law. Any person possessing, taking, disseminating, transferring, or sharing obscene, pornographic, lewd or otherwise illegal images, photographs, or communications will be reported to law enforcement and/or other appropriate state or federal agencies, which may result in arrest, criminal prosecution, and inclusion on sexual offender registries.

Acceptable Use of File Sharing Technology

Employees and students may choose to use file sharing/storing technology (Google Docs, Ever Note, etc.) in connection with school learning or business. Individuals who choose to use such technology are required to follow all other district technology and acceptable use protocols, as well as adhere to the specific guidelines in this policy.

Individuals using file sharing/storing technology in connection with their association with the technology center are expressly prohibited from using the technology in a malicious manner or in any way which violates this or other district policies.

The Superintendent is responsible for regularly reviewing all contracts with potential file sharing/storing technology vendors to ensure the technology centers interests are safeguarded. This responsibility includes making arrangements with vendors which ensure:

- the technology center maintains appropriate ownership of all data connected with the district
- data connected with the district is stored in a secure manner
- data connected with the district will not be used to market to students
- users (or parents) will not be required to waive their rights in order to create an account

<u>District Data</u>

District data encompasses all school records. This information may include:

- information which is protected by FERPA or HIPAA
- confidential information such as home addresses, phone numbers, social security numbers, license numbers, dates of birth, and banking account numbers
- disciplinary or grievance information
- information about criminal investigations, including SRO records and notes
- safety sensitive information, including building layouts, evacuation routes, crisis response plans, etc.

- confidential or attorney client privileged information

District data may only be shared or stored with a file sharing/storing vendor after the board has approved an agreement, recommended by the Superintendent, with the vendor.

Other Data

Other data encompasses all other types of school-related data such as routine documents for individual use or shared items for collaboration projects. Other data may be shared or stored with the district's approved file sharing/storing vendor or on another platform at the discretion of the user.

All Data

Regardless of whether district data or other data is involved, file sharers specifically agree not to share or store files which contain malware, viruses, worms, etc.

Questions regarding whether information is acceptable for file sharing/storing technology should be directed to The Superintendent at the Technology Center main campus. Any individual who discovers that information has been improperly shared or stored is required to promptly notify the Superintendent of the violation. Individuals who violate this policy are subject to disciplinary action as outlined in district policies.