COMPUTER, NETWORK, INTERNET AND OTHER TECHNOLOGY ACCEPTABLE USE

The District recognizes that access to and use of technology in school gives students and staff greater opportunities to learn, engage, communicate and develop skills that will prepare them for work, life and citizenship. The District is committed to helping staff and students develop 21st-century technology and communication skills. To that end, the District provides access to technologies for student and staff use. The following are guidelines and rules that users are expected to follow when using District technologies or when using personally-owned devices in the District.

The District's computers, network, internet and other technologies are intended solely for use in the District's operations, to serve its goals as an educational institution and are intended for educational and work-related purposes only. The District's computers, network, internet and other technologies do not constitute a public access service or public forum. The District has the right to place restrictions on the material accessed and/or posted through the use of its computers, network, internet and other technologies. Use of the District's computers, network, internet and other technologies is a privilege, not a right for students, faculty and staff. The District administrative staff retains the right to collect and/or inspect District computers, network and other technologies at any time, including via electronic remote access; and to alter, add or delete installed software or hardware.

A. Technologies Covered

Technologies covered under this Acceptable Use Policy include, but are not limited to: the internet; District network, computers, mobile devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, webpages, voicemail and fax machines. As new technologies emerge, the District may attempt to provide access to them. Any access provided to new technologies shall be included and/or encompassed under this Acceptable Use Policy.

1. Web Access

The District provides its users with access to the internet, including web sites, resources, content and online tools. That access is restricted in compliance with CIPA regulations and Board policies. Web browsing may be monitored and web activity records may be retained indefinitely. Users

are expected to respect that the web filter is a safety precaution and shall not circumvent it when browsing the Web. If a site is blocked and a user believes it should not be, the user shall follow protocol to alert an IT staff member or submit the site for review. If a site is not blocked and a user believes it should be, the user shall follow protocol to alert an IT staff member or submit the site for review. The District acknowledges that no blocking or filtering mechanism is capable of stopping all inappropriate content all of the time. The best filtering system is good supervision of student technology use and appropriate work-related use by staff.

2. Email

The District may provide users with email accounts for the purpose of District related communication. Availability and use may be restricted based on Board policies. If users are provided with email accounts, they shall be used with care. Users shall not send personal information; shall not attempt to open files or follow links from unknown or untrusted origins; shall use appropriate language; and shall only communicate with other people as allowed by Board policies. Users are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline. Email usage will be maintained and archived. District e-mail communication may be subject to public records requests under the law. Communication over District networks is not considered private, and there shall be no expectation of privacy for any messages sent or received via the District e-mail system.

3. Ownership

The District retains sole right of possession and/or ownership of District equipment and resources, including, but not limited to: District computers, network and other technologies such as materials, software and programs owned by and/or installed on District computers, network and other equipment. The District grants permission to students and staff to use District equipment and resources for educational purposes only, according to the guidelines set forth in this document; the student and staff handbooks; District rules and/or policies; and all applicable laws. Users shall abide by the same Acceptable Use Policies when using District equipment and/or resources off the District's network. Users are expected to treat District equipment and resources with care. Users shall report any

loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse and could be disciplined in accordance with Section H of this Acceptable Use Policy. Use of District equipment and/or resources, including use of the District's network, will be monitored.

B. Social Media

1. Social / Web 2.0 / Collaborative Content

The District recognizes that collaboration is essential to education and may provide users with access to social media web sites or tools that allow communication, collaboration, sharing and messaging. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline, to follow the terms of agreement of each website or service and to comply with Board policies. Posts, chats, sharing and messaging may be monitored. Users shall be careful not to share personally-identifying information online.

2. Staff Use of Social Media for Official Communication

Staff using social media accounts representing the District or District sponsored activities, must be approved by, and registered with the Public Relations Coordinator and the appropriate administrator responsible for each function. Only the appropriate administrator responsible for each function (or his/her designee) has permission to communicate via social media on behalf of the District or District sponsored activities.

Responsibilities of staff maintaining officially sanctioned District social media accounts include, BUT are not limited to, the following:

i. Define the purpose and use of the social media account. This must include a statement of purpose which defines what, if any, restrictions may be placed upon comments, interactions and sharing. The statement of purpose should be available on a District website or on the social media profile if possible.
ii. Maintain transparency, openness, visibility and accountability.

iii. Inform the Public Relations Coordinator of all social media sites used to represent the District or schools and provide access to these sites when requested.
iv. Consider all electronic communication to be a matter of public record.
v. Maintain a high standard of professional communication, use correct grammar and tone, choose appropriate subject matter, courteous words and follow best practices of the social media account.
vi. Use good judgment in all situations.
vii. Follow the District Privacy Policy, this Acceptable Use Policy and all other Board policies when using social media.
viii. District staff shall discuss only school related matters that are within their area of responsibility and within the approved purpose and use of the social media account.
ix. Respect brand, trademark, copyright information and/or images of the District as applicable.
x. Staff may use photos and video (products, etc.) that are available on the District's website and shall follow District Policy 447.5, Photographing, Filming and/or Videotaping of Students in the School, relative to using pictures of students.
xi. Social media account representatives shall not publish or transmit personal information of students, parents and/or staff.
xii. Follow the printed terms and conditions of the social media site when using Twitter, Facebook and other tools.
xiii. Check the reliability and appropriateness of any content shared on social media sites and follow the same rules detailed in Board Policy 381.4, Creation and Maintenance of Internet Websites.

3. Guidelines for Social Media Use by Staff and Students

While social networking is valuable, there are some risks to keep in mind when using these tools. In the social media world, the lines are blurred between what is public or private and personal or professional. These guidelines are intended to inform and guide responsible use of social media and help students and staff understand how to keep the boundaries between personal and professional/ scholastic lives separate.

Staff and students using social media shall follow these guidelines:

i. Staff and students using social media for school purposes shall maintain separate accounts to avoid the issue of blurred boundaries.
ii. Regardless of privacy settings, users should assume that all of the information they have shared on social media is public information.
iii. District staff shall consider their affiliation with the District and the role/position they hold; their comments and opinions may be associated with the District.
iv. Do not publish, post, or release information that is considered confidential or not public. If it seems confidential, it probably is. Online "conversations" are never private.
v. Consider carefully student and staff interactions on private social media accounts. It is recommended that Staff not friend or follow students on social media. District approved sites or pages are preferred and provide openness, visibility and accountability.
vi. Consider carefully the use of private text messaging with students. Preferably, staff shall use online automated text services provided by the District or private companies to text students for official District communication and not personal accounts.

Staff and students may be disciplined for social media activities on District computers, network, internet, or other technologies that are in violation of this Acceptable Use Policy or other Board policies; and/or social networking activities that cause material and substantial disruption to the District's environment, interfere with the rights of others, or present a threat to the health and safety of students, employees and visitors on the District's premises.

C. Rules Governing Use of District Computers, Network, Internet and Other Technologies

1. Prohibited Acts

No District student, faculty, staff member or guest shall:

i. Do anything illegal or anything that adversely affects the District's legal interests, the educational needs of its students, or the efficiency of District operations.

ii. Access or attempt to access accounts or systems, other than the user's own accounts or systems, or an account or system that the user has not been explicitly authorized to access.

iii. Access, view, download, create or disseminate child pornography, obscenity, or things that are harmful to minors.

iv. Engage in the dissemination or solicitation of sexually oriented messages or images.

v. Access, view, download, create or disseminate any material that is libelous, indecent, vulgar, profane or lewd.

vi. Access, view, download, create or disseminate material about products or services that are inappropriate or illegal for minors, including, but not limited to, products or services that are prohibited by law from possession or use by minors.

vii. Use of the District's computers, network, internet, or other technologies to harass, dis, flame, denigrate, impersonate, out, trick, exclude, cyberstalk, or any other activity that is considered to be cyberbullying and/or is in violation of the District's Policy on Nondiscrimination, Anti-Harassment, and Anti-Bullying (111).

viii. Arrange or agree to meet with someone online; distribute to others personally-identifiable information (including phone numbers, addresses, social security numbers, birthdays, credit card numbers, financial information, etc.), any personal information about others, or share personal user accounts and passwords.

ix. Use, possess, copy, or attempt to distribute illegal or unauthorized copies of software or other digital media. This includes software or other digital media in the user's possession or being used without appropriate registration or licensing, or in violation of any trademark or copyright restrictions.

x. Download, attempt to download and/or run unknown or unauthorized programs over the District network or onto District resources without express permission from IT staff. For the security of the District network, such files may only be downloaded from reputable sites and only for educational purposes. Users must register all software, including software downloaded from the internet, that they use in classes or on District devices with IT staff. Users may not make copies of software without the permission of the copyright holder.

xi. Use or download encryption software from any access point within the District's network.

xii. Alter, modify, corrupt, vandalize, or otherwise harm hardware devices belonging to the District or software stored thereon.

xiii. Disable, attempt to disable, or circumvent the District's filtering system or software.

xiv. Engage in, and/or willfully or negligently allow others to engage in, a Denial of Service attack on the District's network or any other host on the internet.

xv. Do anything that could get any portion of the District's internet protocol address put on a Realtime Black List, or perform activities that would cause portions of the internet to refuse to route traffic to any portion of the District's network.

xvi. Perform actions that cause an unusual load on the District's servers that cause slowness or denial of service to other District students, faculty, or staff members.

xvii. Attempt to hack or access sites, servers, accounts, or content that is not intended for student use.

xviii. Send unsolicited commercial e-mail, unsolicited mass mailings, spam, or flood usenet discussion or newsgroups.

xix. Use the District network for personal financial gain, commercial and/or political purposes.

xx. Plagiarize (or use as their own, without citing the original creators) content, including words or images, from the internet. Users shall not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the internet shall be appropriately cited, giving credit to the original authors.

The foregoing list is not exclusive and should not be considered a license to commit other illegal, disruptive, or non-educational activities that are not specified.

2. Netiquette

Users shall:

i. Always use the internet, network resources and online sites in a courteous and respectful manner.

ii. Recognize that among the valuable content online some content maybe unverified, incorrect, or inappropriate. Users shall use trusted sources when conducting research via the internet.
iii. Remember not to post anything online that they would not want parents, staff, or future colleges or employers to see.
iv. Use District technologies for District-related activities and research.
v. Follow guidelines of respectful, responsible behavior online that are expected offline.
vi. Treat District resources carefully and alert an appropriate staff member if there is any problem with their operation.
vii. Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
viii. Students shall alert a teacher, appropriate staff member and District staff shall notify the Director of Human Resources if there is threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
ix. Use school technologies at appropriate times, in approved places, for educational purposes only.
x. Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
xi. Recognize that use of school technologies is a privilege and treat it as such.
xii. Be cautious to protect the safety of other users and self.
xiii. Help to protect the security of District resources.

D. Personally-Owned Devices

Students may use personally-owned devices (including laptops, tablets, smartphones and cell phones), with the permission of teaching staff and may use them in accordance with Board/building policies—unless such use interferes with the delivery of instruction or creates a disturbance in the educational environment.

There is no expectation of privacy for staff and students using personally-owned devices on the District's network. Any misuse of personally-owned devices in violation of Board policies may result in disciplinary action. Therefore, proper netiquette and adherence to the Acceptable Use Policy shall always be used.

E. Security

Users are expected to take reasonable safeguards against the transmission of security threats over the District network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If users believe a District owned computer or mobile device might be infected with a virus, they shall alert IT. Users shall not attempt to remove the virus themselves or download any programs to help remove the virus. All privately owned devices used on the District network must have current anti -virus software installed when applicable.

The District has installed internet filtering software and other safety and security mechanisms. Objectionable and/or harmful words and images, as determined by the District, may be filtered and users may be denied access to them. The activity of students using the District's computers, network, internet and other technologies will be monitored as closely as reasonably possible. The District will make every reasonable effort to ensure that students are under supervision, but it will not be possible to constantly monitor each student. Students may encounter inappropriate information or information that is without educational value. If this occurs, the student shall terminate the activity and report the information to supervisory personnel.

F. Personal Safety

If users see a message, comment, image, or anything else online that makes them concerned for their personal safety, they shall immediately bring it to the attention of an administrator or other appropriate staff member.

Users shall carefully safeguard the personal information of themselves and others.

G. Limitation of Liability

No warranties, expressed or implied, are made by the District for the computers, network, internet and other technology access provided. The District is not responsible for damage or harm to persons, files, data, hardware; delays; non-deliveries; misdeliveries; or service interruptions. While the District employs filtering and other safety and security mechanisms and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. Individual users are solely responsible for making backup copies of their data. The District is not

responsible for the accuracy of information that user's access on the internet and is not responsible for any unauthorized charges students or staff may incur as a result of their use of the District's computers, network, internet and other technologies. Any risk and/or damages resulting from information obtained from the District's computers, network, internet and other technologies is assumed by and is the responsibility of the user. The District will not be responsible, financially or otherwise, for unauthorized transactions conducted over the District's network.

H. Authorization of Use.

All users must have a signed Acceptable Use Policy form on file before they are allowed to use the district's technology systems (including the Internet) independently. Teachers may demonstrate use of the Internet in the classroom, but are responsible for ensuring that students have appropriate forms signed by their parent(s)/guardian(s) before allowing them to use the district's technology systems (including the Internet) independently. Similarly, directors, managers, and supervisors are responsible for ensuring that staff have read and signed the appropriate forms before permitting the independent use of the district's technology systems (including the Internet).

All staff will receive an annual notice reminding them of these policies. For staff, occasional personal use of the Internet and the district e-mail system is permitted, but limited to times which do not interfere with the user's responsibilities.

I. **Violations of this Acceptable Use Policy**

The discovery of misuse of the District's computers, network, internet or other technologies and/or violations of this Policy, whether such discovery is intentional or accidental, will result in application of this Policy; and for illegal activities, referral of the person responsible for the misuse or violation to the appropriate law enforcement authorities for investigation and possible prosecution. Disciplinary actions may include, but are not limited to the following:

Possible disciplinary actions for students:

i. Suspension of network, technology and/or computer privileges;
ii. Notification to parents;
iii. Detention or suspension from school and/or school-related activities; and/or
iv. legal action and/or possible prosecution.

Possible disciplinary actions for staff:

i. Suspension of network, technology and/or computer privileges;
ii. Suspension and/or termination of employment; and/or
iii. legal action and/or possible prosecution.

LEGAL REF.: Chapter 943.70, Wisconsin Statute § 19.35 (2)

CROSS REF.: 831, Use of School District Equipment
771, Reproduction of Materials/Copyright Law
111, Nondiscrimination, Anti-Harassment, and Anti-Bullying

ADOPTED: August 24, 1998

REVISED: October 26, 1998
January 11, 1999
June 10, 2002
October 10, 2005
June 24, 2013
June 9, 2014