School District of Poynette

STAFF

Acceptable Use Policy for Technology Resources

7540.04 - **STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY**

District technology resources (see definition in Bylaw 0100) may be used for incidental personal, non-work-related purposes that do not interfere with the employee's performance of his/her job responsibilities, do not result in direct costs to the District, do not affect other users' use of the resources for education and work-related purposes, do not expose the District to unnecessary risks, or violate applicable Board policies, administrative guidelines, or law/regulations in accordance with Policy 7544, Policy 7540.04, and Policy 7530.02.

Use of District technology resources is a privilege, not a right. When using District technology resources, staff members must conduct themselves in a responsible, efficient, ethical, and legal manner. Staff members found to have engaged in unauthorized or inappropriate use of District technology and/or information resources, including any violation of these guidelines, may have their privilege limited or revoked, and may face further disciplinary action and/or civil criminal liability (see Sec. 943.70, Wis. Stat. (Computer Crimes), Sec. 947.0125, Wis. Stat. (Unlawful Use of Computerized Communication Systems)). Prior to accessing or using District technology and/or information resources, staff members must sign the Staff Technology Acceptable Use and Safety Agreement

This guideline also governs staff members' use of their personal communication devices (PCDs) (as defined by Bylaw 0100) when they are connected to the District's technology resources, creating, using, or transmitting District information resources, or when used while the staff member is on Board-owned property or at a Board-sponsored activity. Staff are reminded that the use of PCDs (including the sending of text messages) may generate a public record or an education record that needs to be maintained in accordance with the Board's record retention schedule and/or Federal and State law.

Below is a non-exhaustive list of unauthorized uses and prohibited behaviors. This guideline further provides a general overview of the responsibilities users assume when using District technology and/or information resources.

A. All use of District technology and/or information resources must be consistent with the educational mission and goals of the District.

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

C. No user may have access to another's private files. Any attempt by users to access another user's or the District's non-public files, or phone or e-mail messages is considered theft. Any attempts to gain access to unauthorized resources or data/information either on the District's computer or telephone systems or any systems to which the District has access are prohibited. Similarly, staff members may not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, or misrepresent other users on the District's network.

D. Staff members may not intentionally disable any security feature used on District technology resources.

E. Staff members may not use District technology resources or their personal communication devices to engage in vandalism, "hacking", or other illegal activities (e.g., software pirating, intellectual property violations; engaging in slander, libel or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; sale of illegal substances or goods.

    1. Slander and libel - In short, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Staff members shall not knowingly or recklessly post false or defamatory information about a person or organization. Staff members are reminded that material distributed over the Internet is "public" to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people and harmful and false statements will be viewed in that light.

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

3. Vandalism and Hacking – Deliberate attempts to damage the hardware, software, or data/information residing in District technology resources or any computer system attached through the Internet is strictly prohibited. In particular, malicious use of District technology resources to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system is prohibited.

   Attempts to violate the integrity of private accounts, files, or programs, the deliberate infecting of the network or computers, laptops, tablets, etc., attached to the network with a "virus", attempts at hacking into any internal or external computer systems using any method will not be tolerated.

   Staff members may not engage in vandalism or use District technology resources or their personal communication devices in such a way that would disrupt others' use of District technology resources.

   Vandalism is defined as any malicious or intentional attempt to harm, steal, or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network security and/or the Board's technology protection measures. Staff members also must avoid intentionally wasting limited resources. Staff members must immediately notify the building principal or direct supervisor if they identify a possible security problem. Staff members should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

4. Use of District technology resources to access, process, distribute, display or print child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that depicts, describes or represents in a patently offensive way with respect 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; and material that lacks serious literary, artistic, political or scientific value as to minors. If a staff member inadvertently accesses material that is prohibited by this paragraph, s/he should immediately disclose the inadvertent access to the building principal or direct supervisor. This will protect the user against an allegation that s/he intentionally violated this provision.

5. Unauthorized Use of Software or Other Intellectual Property from Any Source – Laws and ethics require proper handling of intellectual property. Software is intellectual property, and, with the exception of freeware, is illegal to use without legitimate license or permission from its creator or licensor. All software loaded on District computers must be approved by the Director of Technology, and the District must own, maintain, and retain the licenses for all copyrighted software loaded on District computers. Staff members are prohibited from using District technology resources for the purpose of illegally copying another person's software. Illegal peer-to-peer file trafficking of copyrighted works is prohibited.

   Online articles, blog posts, podcasts, videos, and wiki entries are also intellectual property. Staff members should treat information found electronically in the same way they treat information found in printed sources - i.e., properly citing sources of information and refraining from plagiarism.

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

G. District technology resources may not be used for private gain or commercial purposes (e.g., purchasing or offering for sale personal products or services by staff members), advertising, or political lobbying or campaigning is prohibited. This provision shall not limit the use of District technology resources by staff members for the purpose of communicating with elected representatives or expressing views on political issues.

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

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through or utilizing District technology resources. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive, or disrespectful language in communications made through or utilizing District technology resources (including, but not limited to, public messages, private messages, and material posted on web pages).

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

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

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

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

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

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

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

K. Users have no right or expectation to privacy when using District technology and/or information resources. The Board reserves the right to access and inspect any facet of its technology and/or information resources, including, but not limited to, computers, laptops, tablets, and other web-enabled devices, networks or Internet connections or online education services or apps, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein. A staff member's use of District technology and/or information resources constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the technology resources and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technology monitoring systems and staff monitoring, may lead to discovery that a staff member has violated Board policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a staff member has violated Board policy and/or law, or if requested by local, State or Federal law enforcement officials. Staff are reminded that their communication is subject to Wisconsin's public records laws and FERPA (See Policy 8330).

The following notice will be included as part of the computer log-on screen:

"District technology resources (including computers, laptops, tablets, e-readers, cellular/mobile telephones, smartphones, other web-enabled devices, video and/or audio recording equipment, projectors, software and operating systems that work on any device, copy machines, printers and scanners, information storage devices (including mobile/portable storage devices such as external hard drives, CDs/DVDs, USB thumb drives and memory chips), the computer network, Internet connection, and online educational services and apps) are to be used for educational and professional purposes only. Users are reminded that all use of District technology resources, including Internet use, is monitored by the District and individual users have no expectation of privacy."

L. Use of the Internet and any information procured from the Internet is at the staff member's own risk. The Board makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through District technology resources will be error-free or without defect. The Board is not responsible for any damage a user may suffer, including, but not limited to, loss of data, service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of information obtained through the Internet. Information (including text, graphics, audio, video, etc.) from Internet sources used in class should be cited the same as references to printed materials. The Board is not responsible for financial obligations arising through the unauthorized use of its technology resources. Staff members will indemnify and hold the Board harmless from any losses sustained as the result of the staff member's misuse of District technology resources.

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

N. Proprietary rights in the design of websites/services/apps hosted on the Board-owned or leased servers remains at all times with the Board without prior written authorization.

N. Staff members own the copyright to works created outside the scope of their employment responsibilities and without the use of Board resources. Staff members may post such work on the District website to facilitate access by students and/or staff. Notice of such posting and claim of ownership must be provided to the building principal. By posting such work on the District's website, the staff member agrees to grant a non-exclusive license or permission for any staff or

student within the District to freely use such work. The Board shall own the copyright on any works created by staff members within the scope of their employment responsibilities.

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

P. File-sharing is strictly prohibited. Staff members are prohibited from downloading and/or installing file-sharing software or programs on District technology resources.

Q. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the District's users will be fully investigated and disciplinary action will be taken as appropriate.

R. Preservation of Resources: District technology resources are limited. Each staff member is permitted reasonable space to store email, web, and personal school/work-related files. The Board reserves the right to require the purging of files in order to regain disk space.

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

    1. Websites with extensive commercial advertising may be included on the District or classroom websites/services/apps or designated as a required or recommended site only if there is a compelling educational reason for such selection.

    2. Staff members may make use of high-quality, unbiased online educational materials that have been produced with corporate sponsorship. Staff members may not make use of educational materials that have been developed primarily for the purpose of promoting a company and/or its products or services.

Abuse of Network Resources

Peer-to-peer file sharing, mass mailings, downloading of unauthorized games, videos, and music are wasteful of limited network resources and are forbidden. In addition, the acquisition and sharing of copyrighted materials is illegal and unethical.

Unauthorized Printing

District printers may only be used to print school/work-related documents. Printers, like other school resources, are to be used in a responsible manner. Ink cartridges and paper, along with printer repairs and replacement are very expensive. The District monitors printing by user. Print jobs deemed excessive and abusive of this privilege may result in charges being assessed to the staff member.

Any questions and concerns regarding these guidelines may be directed to the Superintendent.

Revised 11/23/15

Revised 3/18/16

Legal

943.70, Wis. Stat.

947.0125, Wis. Stat.

Family Educational Rights and Privacy Act of 1974, as amended

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

18 U.S.C. 2256A

18 U.S.C. 1460

18 U.S.C. 2246

20 U.S.C. 677

20 U.S.C. 9134 (2003)

School District of Poynette

Acceptable Use Policy for Technology Resources
Staff User Policy Acknowledgement

Please read the following information carefully before signing this document. All sections of this contract must be signed by staff member. *[Technology policies are available on our district's website or in print upon request]*

STAFF: As a staff member of the School District of Poynette, I have read the district's Acceptable Use Policy (AUP) and this policy acknowledgement. I am aware that the AUP and all of its terms and conditions are included in this contract. I understand that my access to technology resources is designed for educational purposes. I understand that my violation of the district's AUP will result in the temporary or permanent loss of Internet and/or network access, as well as other disciplinary action.

Name (Please Print): _____

Signature: _____**Date:** ____/_____/____