

Technology Acceptable Use and Safety Form

Staff Form



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

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

- A. Staff members are responsible for their behavior and communication using the Ed-Tech. All use of the Education Technology must be consistent with the educational mission and goals of the District.
- B. Staff members may only access and use the Education Technology by using their assigned account and may only send school-related electronic communications using their District-assigned email addresses. Use of another person's account/e-mail address/password is prohibited. Staff members may not allow other users to utilize their passwords. Staff members may not go beyond their authorized access. Staff members are responsible for taking steps to prevent unauthorized access to their accounts by logging off or "locking" their computers/laptops/tablets/personal communication devices when leaving them unattended.
- C. Staff members may not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, or misrepresent other users on the District's network. Staff members may not intentionally disable any security features of the Ed-Tech.
- D. Staff members may not use the Education Technology to engage in "hacking" or other illegal activities (e.g., software pirating, intellectual property violations; engaging in slander, libel or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; sale of illegal substances or goods.
 - 1. Slander and libel are terms defined specifically in law. Generally, slander is "oral communication of false statements injurious to a person's reputation," and libel is

Technology Acceptable Use and Safety Form

Staff Form



"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 the Education Technology to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex, sexual orientation or transgender identity, age, disability, religion or political beliefs. Sending, sharing, viewing or possessing pictures, text messages, e-mails or other materials of a sexual nature (i.e., sexting) in electronic or any other form, including the contents of a personal communication device or other electronic equipment, is grounds for discipline, up to and including termination. Such actions will be reported to local law enforcement and child services as required by law.
- E. Transmission of any material in violation of any State or Federal law or regulation, or Board policy is prohibited.
- F. Any use of the Ed-Tech for commercial purposes, advertising, or political lobbying is prohibited.
- G. Staff members are expected to abide by the following generally accepted rules of online etiquette:
1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the Board's Education Technology. Refrain from using obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.
 2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.
 3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a staff member is told by a person to stop sending him/her messages, the staff member must stop.

Technology Acceptable Use and Safety Form

Staff Form



4. Do not post information that, if acted upon, could cause damage or danger of disruption.
 5. Never reveal names, addresses, phone numbers, or passwords of students while communicating on the Education Technology, unless there is prior written parental approval or it is otherwise permitted by Federal and/or State law.
 6. Check e-mail, at least daily per employee handbooks. Nothing herein alters the staff member's responsibility to preserve e-mail and other electronically stored information that constitutes a public record, student education record and/or a record subject to a Litigation Hold.
- H. Use of the Education Technology to access, process, distribute, display, or print child pornography and other material which is obscene, objectionable, inappropriate or harmful to minors are prohibited. For example, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that depicts, describes, or represents in a patently offensive way with respect 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. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the Board's computers/network (e.g., viruses) are also prohibited.

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

- I. Malicious use of the Board's Education Technology to develop programs that harass other users or infiltrate a computer/laptop/tablet or computer system and/or damage the software components of a computer or computing system is prohibited. Staff members may not engage in vandalism or use the Ed-Tech in such a way that would disrupt its use by others. Vandalism is defined as any malicious or intentional attempt to harm, steal or destroy data of another user, school networks, or technology hardware. This includes but is not limited to uploading or creation of computer viruses, installing unapproved software,

Technology Acceptable Use and Safety Form

Staff Form



changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass Network security and/or the Board's technology protection measures. Staff members may not use the Board's Ed-Tech in such a way that would disrupt their use by others. Staff members should refrain from intentionally wasting limited resources.

- J. All communications and information accessible online should be assumed to be private property (i.e, copyrighted and/or trademarked). All copyright issues regarding software, information, and attributions of authorship must be respected.
- K. Downloading of information onto school-owned equipment or contracted online education services is prohibited, without prior approval from Technology Director. If a staff member transfers files from information services and electronic bulletin board services, the staff member must check the file with a virus-detection program before opening the file for use. Only public domain software may be downloaded. If a staff member transfers a file or software program that infects the District's Ed-Tech with a virus and causes damage, the staff member will be liable for any and all repair costs to make the Education Technology once again fully operational.
- L. Staff members have no right or expectation to privacy when using the Education Technology. The District reserves the right to access and inspect any facet of the Ed-Tech, including, but not limited to, computers, laptops, tablets, personal communication devices, networks or Internet connections or online education services, e-mail or other messaging or communication systems or any other electronic media within its technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message or material of any nature or medium that may be contained therein. A staff member's use of the Ed-Tech constitutes his/her waiver of any right to privacy in anything s/he creates, stores, sends, transmits, uploads, downloads or receives on or through the EdTech and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technical monitoring systems and staff monitoring, may lead to a discovery that a staff member has violated Board policy and/or the law. An individual search will be conducted if there is reasonable suspicion that a staff member has violated Board policy and/or law, or if requested by local, State or Federal law enforcement officials. Staff is reminded that their communication is subject to Wisconsin's public records laws and FERPA (See Policy 8330). The use of passwords does not guarantee confidentiality, and the Board retains the right to access information in spite of a password.
- M. Use of the Internet and any information procured from the Internet is at the staff member's own risk. The Board is not responsible for any damage a user suffers, including loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions. The Board is

Technology Acceptable Use and Safety Form

Staff Form



not responsible for the accuracy or quality of information obtained through its services. Information (including text, graphics, audio, video, etc.) from Internet sources used in class should be cited the same as references to printed materials. The Board is not responsible for financial obligations arising through the unauthorized use of the Ed-Tech. Staff members will indemnify and hold the Board harmless from any losses sustained as the result of misuse of the Ed-Tech by the staff member.

- N. Disclosure, use and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent on the "Student Education Technology Acceptable Use and Safety Agreement Form."
- O. Proprietary rights in the design of websites hosted on the Board-owned District-affiliated or leased servers remains at all times with the Board without prior written authorization.

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

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

Signature

Name: _____

Signature: _____

Date: _____