School District of Shorewood
363.1 Exhibit (1)
Student and Staff Acceptable Use of District Network Agreement

Use of electronic devices and network in the Shorewood School District is a privilege that should be used to support learning appropriate for school. The smooth operation and maintenance of the system(s) relies on users adhering to established guidelines.

By signing this acceptable use agreement (AUP):

1. Users acknowledge that they have read the terms and conditions of acceptable Use Policy (AUP) and guideline, and understand the inherent responsibilities.
2. The requester and his/her parent(s)/guardian(s) should be aware that the Shorewood School District does not have control of the information on the Internet, but takes measures possible to protect our children through internet filtering and education of ethical and appropriate use. Some sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people.
3. By signing this agreement, students and parent(s)/guardian(s) agree to abide by the restriction outlined in this policy and guideline. The student and his/her parent(s)/guardian(s) of minors are responsible for setting and conveying the standards that their child should follow. Failure to return this agreement with signatures of both the user and parent/guardian will result in denial of access to the network.

I have read and understand the terms of the Shorewood School District AUP and guideline, and agree to those terms. I hereby give permission to issue and account for my child and certify that the information contained on this form is correct.

_____ _____

Parent/Guardian Signature Date

School District of Shorewood

363.2 Guideline

Acceptable Use of Technology

The Board of Education believes the use of electronic devices and network in the Shorewood School District is a privilege that should be used to support learning appropriate for school. It allows people to become a community of learners who live and work productively in the changing digital age. It is our district belief to provide technology resources for our district community to promote educational excellence and operational efficiency through resource sharing, innovation and communication. The smooth operation and maintenance of the system(s) relies on users adhering to established guidelines.

The District's Computer Systems are used for educational purposes only and in the interests of the District. All equipment, software, messages and files are the exclusive property of the District. The User of the Shorewood School District's computers and network systems bears the ultimate responsibility to the adherence of the acceptable use of technology.

Access

As a User of technology, the User understands and agrees:

- that computer use is monitored electronically by Shorewood staff.
- that using the computer systems for non-educational purposes in violation of District Policy is strictly prohibited.
- not to use the computer systems in a way that is disruptive, offensive, or harmful to the User, others or to the District.
- not to use a password that has not been disclosed to the District or to share or disclose my password with others.
- not to use passcodes, access a file or retrieve any stored communication, other than where authorized, unless there has been prior clearance by a teacher or District administrator.
- not to copy, send or receive copyrighted or confidential materials without permission.
- The principal or designee or other system supervisor reserves the right to deny access to any person who is in violation of the use of the district technology systems.

Technology has changed the ways in which information is accessed, communicated, and transferred in society. The Board of Education provides students, teachers and staff with access to computers, software, the Internet and other electronic resources for educational purposes. The objective of these purposes are to utilize online resources to enhance the instruction and content creation for students. Educators will continually adapt their means and methods of instruction, and the way they approach student learning to incorporate the vast, diverse, and unique resources available through the Internet.

Appropriate Use

Employees, students and community are expected to act in a responsible, ethical and legal manner in accordance with this policy, accepted rule of network etiquette, and federal and state law.
Specifically, the following uses are prohibited from:

- using of the network or District network for personal or non-education related purposes. Examples include use of email for non-educational related information and social networking sites for personal information.

- storing of personal files, personal digital photographs and music on district servers as storage space is limited and intended for school-related data.
- interfering with the work of other users of the system. Examples include tampering with files, data or passwords of other users; and destroying, modifying or abusing hardware or software.
- impersonating of another user.
- installing of illegal and/or inappropriate or copyrighted software or software components designed to damage the hardware or software of a computing system ("hacking").
- using of the network for commercial or non-profit purposes and advertisement.
- using the network for participating in illegal activity, making discriminatory remarks, using profanity or inappropriate offenseive language, or accessing obscene/pornoprgahpic material.
- unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials.
- damage to or modification of network hardware or software.

Website Safety

Due to the ever changing information available through the Internet, the District permits responsible and safe use of additional publicly accessible tools for instructional and educational purposes. Users are expected to engage in safe and acceptable use of the Web resources at all times, including limiting one's disclosure of personal information over the Web. Falsifying an identity or using someone else's identity is a violation of District policy and state law (Section 943.70, Wis. Stats.) which may result in disciplinary or criminal action against the violator.

Staff members will monitor the online activities of students while at school. Monitoring may include, but is not necessarily limited to, visual observations of online activities; or use of specific monitoring tools to review browser history and network, server, and computer logs.

Students, teachers and staff shall not access social media for personal use from the District's network, but shall be permitted to access social media for education.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users of the District's Educational Technology are personally responsible and liable, both civilly and criminally, for uses of the Educational Technology not authorized by this Board policy and its accompanying guidelines.

The Board designates the Superintendent, the Director of Technology and the administrative staff as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of the District's Education Technology.

Non-District-Provided Technology

The District permits use of personal technology devices and the District's Wireless Public Network by students and staff in support of teaching and learning. Unlimited use of personal devices is permitted so long as it does not interfere with educational or employment responsibilities and as long as the use does not hinder, disrupt or consume

an unreasonable amount of network or staff resources, violate state or federal law, or violate other District policies, rules or guidelines.

Photographic Capabilities

In accordance with state law (Section 175.22, Wis. Stats., §942.08, §942.09), under no circumstances shall cellphones, tablets, laptops or any other devices with photographic capabilities be used in locker rooms, bathrooms, or other areas where privacy is expected. Devices with photographic capabilities shall not be used to photograph students and others without their permission and shall not be used to photograph any items that are confidential (e.g., testing materials). It is assumed that all pictures of students may be used for educational purposes/publications unless said parent/guardian has signed off to exclude their child from such instances. A student or staff member who violates the photographic capabilities will be subject to the consequences described.

Student Safety

In accordance with requirements of the Children's Internet Protection Act (CIPA)and the Neighborhood Children's Internet Protection Act (NCIPA), all equipment connection to the network from any connection located within the District's buildings will be blocked or filtered. The technology protection filters may not be disabled or by-passed by anyone at any time that students may be using the technology to access online resources. Any student who attempts to disable or by-pass the technology protection measures will be subject to discipline. The District will make best efforts to prevent users from accessing or transmitting visual depictions of material deemed obscene, child pornography, and any material deemed harmful to minors as those terms are defined in CIPA. It will also make best efforts to prevent users from accessing or transmitting offensive, disruptive, or harmful data or any "inappropriate matter" as that term is used in the NCIPA. This includes, but is not limited to, messages, files, or data that contain the following:

- pornographic or erotic images
- sexual implications
- racial slurs
- derogatory gender-specific comments
- information, comments or instructions intended to frighten, intimidate, threaten, abuse, annoy harass or to harm another person(s) or organization(s) that offensively address a person's age sexual orientation, beliefs, political beliefs, genders, religious beliefs, national origin or disability
- any comment which in any way defames, slanders or libels another person(s)

The District acknowledges that no blocking or filtering mechanism is capable of stopping all inappropriate content all of the time, but also understands some material may slip through from time to time. At that point the District will take further action to ensure that does not happen in the future. It is the responsibility of employees to make best efforts to guide and to monitor students in the effective and appropriate use of the District's device and network system. This includes, but is not limited to:

- teaching students how to find educationally appropriate electronic materials and how to judge the educational suitability of electronic materials.
- teaching students information literacy skills, including understanding of safety, copyright and data privacy.
- teaching students ethically responsible and appropriate behavior when accessing and communicating ia the web.
- teaching students proper safety and security procedures when using email, online communities, collaborative workspaces and other forms of electronic communication.

Filter and Monitoring

The Technology Department Personnel may temporarily or permanently unblock access to websites containing appropriate material if access to such sites has been inappropriately blocked. The determination of whether material is appropriate of inappropriate shall be based on the content of material and the intended use of the material, not on the protection actions of the technology protection measure.

The Director of Technology may disable the technology protection measures to enable access for bona-fide research or other lawful purposes.

Parents are advised that a determined User may be able to gain access to services in the Internet that the District has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communication that they and/or their parents may find inappropriate, offensive objectionable or controversial.

Privacy

Any online activity that is considered inappropriate in the classroom is also inappropriate in all uses of online resources. This includes but is not limited to profanity or racist, sexist or discriminatory remarks. The District prohibits users of the District's network from using, accessing, storing or transmitting inappropriate content.

The District utilizes software and/or hardware to monitor online activity of students, teachers and staff to block/filter access to material that is obscene, objectionable, inappropriate and/or harmful to minors. "Harmful to minors" is a term defined by the Communications Act of 1934 (47 U.S.C. 254(h)(7)) as any picture, image, graphic image file, or other visual depiction that includes, but is not limited to offensive, profane, abusive, harassing, sexually explicit, threatening or obscene language or visual depictions, as well as pornography and child pornography.

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, including, but not limited to electronic and voice mail, computer files, and other electronic transmissions contained in or used in conjunction with the District's computer system, telephone system, electronic mail, voice mail system and online resources such as Google Suite, formerly known as Google Apps for Education. All such information files shall be and remain the property of the School District and no User shall have any expectation of privacy regarding such materials.

Review of such information may be done by the District with or without notice or of the student's or staff member's knowledge. The use of passwords does not guarantee confidentiality, and the District retains the right to access information in spite of a password. All passwords or security codes must be registered with the District. A staff member's refusal to permit such access may be grounds for discipline up to and including discharge.

Cyberbullying

The District's computer network and the Internet, whether accessed on campus or off campus, during or after school hours, may not be used for the purpose of harassment. All forms of harassment over the Internet and any network are unacceptable and viewed as the violation of this policy and the District's acceptable use policy and guidelines.

Cyberbullying includes harassing, teasing, intimidating, threatening or terrorizing another person by sending or posting inappropriate and hurtful email or text messages, digital pictures, or Website posting, including blogs and social networking sites. Users are responsible for the appropriateness of the material they transmit on the Internet and/or within the District's network.

The administration shall fully investigate all reports of cyberbullying. Students, employees and community members, who believe they have been the victims of such misuses of technology, as described in this policy and guideline, should not erase the offending material from the system. A copy of the material should be forwarded to, printed, screenshot, etc., and brought to, the attention of any district employee. Disciplinary action may include, but is not limited to, the loss of computer privileges, detention, suspension or expulsion for verified perpetrators of cyberbullying. In addition, when any kind of threat is communicated or when a hate crime is committed, this shall be reported to local law officials.

Email

Computers, electronic mail, and voice mail are to be used for business and educational purposes. Personal messages via Board-owned technology should be limited in accordance with the Superintendent's guidelines. Staff members are encouraged to keep their personal records and personal business at home.

Students and staff members are prohibited from sending offensive, discriminatory, or harassing computer, electronic, or voice mail messages.

In accordance with State law, any staff member who sends an electronic message, whether through email, social media or other forms of online communication, with the intent to frighten, intimidate, threaten, or harass another person or sends a message containing lewd, obscene, or profane language will be subject to appropriate discipline by the District and may be found guilty of a Class D misdemeanor.

When available, the District's e-mail system must be used by employees for any official District e-mail communications. Personal e-mail accounts on providers other than the District's e-mail system may be blocked at any time due to concerns for network security, SPAM, or virus protection. Furthermore, District staff are expected to exercise reasonable judgment and prudence and take appropriate precautions to prevent viruses from entering the District's network when opening or forwarding any e-mails or attachments to e-mails that originate from unknown sources.

Public Records

The District complies with all Federal and State laws pertaining to electronic mail. Accordingly, e-mails written by or sent to District staff and Board members may be public records, or education records if their content includes personally identifiable information about a student.

State and Federal law exempt certain documents and information within documents from disclosure, no matter what their form. Therefore, certain e-mails may be exempt from disclosure or it may be necessary to redact certain content in the e-mails before the e–mails are released pursuant to a public records request, the request of a parent or eligible student to review education records, or a duly served discovery request.

E-mails written by or sent to District staff and Board members by means of their private e-mail account may be public records if the content of the e-mails concerns District business, or education records if their content includes personally identifiable information about a student.

Consequently, staff shall comply with a District request to produce copies of e-mail in their possession that are either public records or education records, even if such records reside on a computer owned by an individual staff member, or are accessed through an e-mail account not controlled by the District.

The District maintains archives of all e-mails sent and/or received by Users of the District's e-mail service. Staff members are required to forward copies of any e-mails received in their personal e-mail account(s) not affiliated with the District server to their District e-mail account so that these records are also archived for future retrieval, if necessary.

Unauthorized E-mail

The Board does not authorize the use of its proprietary computers and computer network ("network") to accept, transmit, or distribute unsolicited bulk e-mail sent through the Internet to network e-mail accounts. In addition, Internet e-mail sent, to or through the network, that makes use of or contains invalid or forged headers, invalid or non-existent domain names, or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit e-mail to be sent to or through the network is unauthorized. Similarly, e-mail that is relayed from any third party's e-mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the e-mail, is also an unauthorized use of the network.

The Board does not authorize the harvesting or collection of network e-mail addresses for the purposes of sending unsolicited e–mail. The Board reserves the right to take all legal and technical steps available to prevent unsolicited bulk e-mail or other unauthorized e-mail from entering, utilizing, or remaining within the network.
The District retains the right to monitor or access any District e-mail accounts at any time. Users should not expect that their communications sent or received through the District e-mail system will remain confidential and personal.

Authorized Use

Students, staff and Board members using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use and safety by signing and submitting the AUP annually.

Consequences

Inappropriate use of the District’s technology resources, Web resources or District property and any other violation of District policies, guidelines or rules may result in suspension of technology privileges, report to criminal authorities, legal action, and discipline up to and including suspension and expulsion for students and discipline up to and including discharge for employees. Specifically, users are notified that sexually explicit or pornographic content has no place in the District and violators who use or access such content will face severe consequences

including expulsion or termination. In addition, violations may result in financial charges for repair, replacement or services, as well as legal action.

Administrators may confiscate and search personal devices while on District property if the administrator has reasonable suspicion that the use of the device or technology is in violation of this Policy. The District will cooperate fully with local, state or federal officials in any investigation related to any illegal activities conducted through the District's systems.

LEGAL REF.: Sections 120.12(1) Wisconsin Statutes
120.13(1)
120.18(1)
175.22
942.08
942.09
943.70
947.0125
955.55 PI 8.01(2)(k)
FEDERAL REF: Children's Internet Protection Act
Protecting Children in the 21st Century Act
Children's Online Privacy Protection Act
E-rate funding requirements
CROSS REF.: 332.4, Distance Education
335, Student Records
350, Selection of Core Curricular Instructional Materials
350.2, Library/Media Center Materials Selection
445 , Student Harassment
512, Employee/Volunteer Harassment
740, Use of Copyrighted Materials
810, Access to Public Records
Operational Expectation 11
APPROVED: February 11, 1997
REVISED: September 21, 2006
March 18, 2008
December 10, 2013
September 13, 2016
June 27, 2017
August 11, 2017