

Policy 6.28 Acceptable Use of District Technology

The School District of Brown Deer provides employees and students with access to the district's telecommunication system which includes but not limited to: desktop and portable computers; file, web, print, and database servers; projection devices; document cameras and interactive whiteboards; software applications; Internet and district websites; email service; and a variety of electronic communication devices (ECD), such as cell phones, pagers, and personal digital assistants (PDAs), that electronically transmit voice and text messages, as well as visual images, between users and provide wireless connectivity for accessing the district's email service, Internet, and voice messages.

For the purpose of this Acceptable Use Policy (AUP), the district defines "users" as all staff, students, faculty, administrators, and other granted access to the district computers and network.

The purpose of the district telecommunication system is to assist staff in preparing to graduate students with 21st Century skills and a sense of purpose to adapt, thrive and excel in a changing world by providing them with electronic access to a wide range of information and the ability to communicate with people from throughout the world. The term "educational purpose" includes use of the system for classroom activities, professional or career development, and limited high-quality self-discovery activities.

Additionally, the system is used to increase district intra-communication, enhance productivity, and assist district employees in upgrading their skills through greater exchange of information with their peers. The district system also assists the district in sharing information with the local community, including parents, social service agencies, government agencies, and businesses.

Users of the district system will follow the School District of Brown Deer Acceptable Use Guidelines and understand clearly that such use is a PRIVILEGE and NOT A RIGHT, such that the district reserves the right to hold users accountable for misuse of the system, including taking disciplinary action or revoking a user's privilege. There should be NO EXPECTATION of privacy by students and staff using District technology. The District will have access to all user accounts, including data created, and will review/monitor technology use as necessary to maintain system integrity and ensure responsible technology use.

Legal References: Sections 118.001, 120.13(1), 943.70(2), and 947.0125 of the Wisconsin Statutes; Children's Internet Protection Act; Neighborhood Children's Internet Protection Act; Children's Online Privacy Act; Federal Copyright Law [17 U.S.C.]; Technology Education and Copyright Harmonization Act (TEACH Act).

Cross Reference(s): Policy 6.28 Guidelines Acceptable Use District Technology
Policy 6.28 Attachment(s) Acceptable Use Guidelines
Policy 6.28 Attachment(s) Letter

Approved: September 27, 1997

Revised: July 27, 2009

Policy 6.28 Guidelines Acceptable Use of District Technology

1. District Limitation of Liability

The district makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the district system will be error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.

2. District Responsibilities

- a. The district Instructional Technology Coordinator (ITC) will oversee the district system and will work under direct supervision of the District Administrator. The district ITC will establish a process for setting up individual network accounts/passwords, set quotas for disk usage if needed, establish a district virus protection process, monitor and maintain a proper internet filter based on Children's Internet Protection Act (CIPA) guidelines, and other activities to ensure effective operation of the system.
- b. The district systems administrator under the direction of the ITC will regularly evaluate the security of the district's computer network and its electronic student records. An annual evaluation, which could include an external audit, will be conducted to measure the adequacy of district network security measures and identify any risks to confidentiality of student records. Findings from the annual evaluation will be reported to the school board.
- c. The building Principal will serve as the building-level coordinator of the district system, will approve building-level activities, ensure teachers receive proper training in the use of the system and the requirements of this policy, establish a system to ensure adequate supervision of students using the system, maintain executed user agreements, and be responsible for interpreting the district Acceptable Use Guidelines at the building level.

3. Access to the System

- a. Elementary Students – Elementary age students (preK-4th) may be given their own network login and passwords to access network resources. If an email account is needed, these students will be granted access only through a classroom account. Any time students are asked to identify themselves online they are to use FIRST NAMES ONLY. No other personal contact information (full name, address, telephone, personal email, age, etc) should be given at any time unless with full permission from parent/guardian. Elementary age students will be taught to not reveal their unique username/password or use another's in an attempt to gain access to the system. Doing so will violate the District's Acceptable Use Policy and have consequences. Users will be granted access upon the annual completion of the appropriate district AUP acceptance form including signature from parent and guardian.
- b. Middle and High School Students – Middle and high school age students (4th – 12th) will be given their own network login and passwords to access network resources including email service. If an email account is needed, these students will be granted access and will be taught proper email etiquette. Any time students are asked to identify themselves online they are to use FIRST NAMES ONLY. No other personal contact information (full name, address, telephone, personal email, age, etc) should be given at any time unless with full permission from parent/guardian if

the student is a minor. Middle and high school age students will be taught to not reveal their unique username/password or use another's in an attempt to gain access to the system. Doing so will violate the District's Acceptable Use Policy and have consequences.

Users will be granted access upon the annual completion of the appropriate district AUP acceptance form including signature from parent and guardian if the student is a minor.

- c. District Employees – District employees will be provided with an individual network and email account and *may* have VPN access to the system. District employees may also be given district portable devices (laptops, Blackberrys/PDAs) which will be connected and secured on the district's wireless network. Any personal equipment attempting to access the district wireless network must first be granted approval from the building principal, district administrator, or Instructional Technology Coordinator and only after the device is inspected for proper and recent virus protection will such access be granted. Any device that then connects to the network will be subjected same level of district monitoring and tracking set forth by the AUP. Devices with WiFi capabilities that do not meet operating system or virus and security requirements will not be permitted on the network.

Users will be granted access upon the annual completion of the appropriate district AUP acceptance form.

- d. Guest Accounts – Guests including but not limited to substitutes may receive an individual account with the approval of a building principal if there is a specific, district-related purpose requiring such access. Use of the system by a guest must be specifically limited to the district-related purpose and may or not include network storage.

Users will be granted access upon the annual completion of the appropriate district AUP acceptance form.

4. Parental Notification and Responsibility

- a. The district will notify parents about the district network and the policies governing its use. Annually, parents must sign the district's AUP acceptance form in order for their student to have any access to the system.
- b. A parent or guardian of a minor child can sign an annual parental denial form requesting that his/her child not have individual access to the Internet.
- c. Parents have the right to request the termination of their child(ren)'s individual account at any time.
- d. In compliance with federal law requirements, an Internet filtering device shall be used on all District computers that access the Internet in an effort to protect against access to visual depictions that are obscene, child pornography or harmful to minors. The District acknowledges that even with a filtering system, complete control and/or access to objectionable material cannot be assured. Some independent users may still discover unsuitable information or have access to materials that are illegal, defamatory, inaccurate or potentially objectionable to some people. The District is not responsible for Internet content, its authenticity and/or its accuracy
- e. In addition, school districts are now also required to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. Information to this effect is required to be addressed as part of a district's Internet safety policy. This law change was included in the Broadband Data Improvement Act (Public Law No: 110-385) signed into law by President George Bush on October 10, 2008.

5. Due Process and Enforcement

- a. The district will cooperate fully with local, state, or federal officials in any investigation concerning to or relating to any illegal activities conducted through the district system.
- b. In the event there is an allegation that a staff member or student has violated the Acceptable Use Guidelines, the following procedure should be followed when appropriate.
 - (1) Notify teacher in charge or supervisor of the employee immediately.
 - (2) School officials will notify Instructional Technology Coordinator for electronic proof/backup that will substantiate the claim.
 - (3) School officials will notify the person with a written or verbal notice of the alleged violation.
 - (4) The accused person will have an opportunity to present an explanation before a neutral administrator before a ruling is announced.
- c. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other board policies or school rules, the violation will be handled according to established procedures.
- d. Employee violations of the Acceptable Use Guidelines will be handled in accordance with district policy.

6. Privacy Rights

- a. System users should have NO EXPECTATION of PRIVACY when using the district system. That is, school officials reserve the right to monitor ever user's use of district's computer system at all times and without notice.
- b. School officials can inspect information stored on its computer system, including all equipment issued to personnel; search and read email stored either on the district's network or contracted provider.
- c. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the Acceptable Use Guidelines, board policy or the law.
- d. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or board policy. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.
- e. District employees should be aware that their personal files are discoverable under state public records laws.
- f. Respect the rights of others to freedom from harassment or intimidation. Users will promptly disclose to instructional staff or a supervisor any message they receive that is inappropriate, constitutes harassment or makes them feel uncomfortable.

7. Copyright and Plagiarism

- a. District policies on copyright will govern the use of material accessed through the district system. Because the extent of copyright protection of certain works found on the Internet is unclear, employees will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement. Teachers will instruct students to respect copyright and to request permission when appropriate.

- b. District policies on plagiarism will govern use of material accessed through the district system. Teachers will instruct students in appropriate research and citation practices.
8. Other Unacceptable Uses
- a. Physical damage or vandalism; modification or theft of equipment.
 - b. Using the network to intimidate, humiliate, or threaten another individual.
 - c. Accessing or storing illegal, sexually explicit or otherwise objectionable material on district file servers. Including but not limited to: games, music, movies/videos.
 - d. Downloading and/or installing any software, free or otherwise, that is not first approved by the building principal or ITC.
 - e. Activities related to soliciting or lobbying for political or religious causes or for unethical or disruptive activities.
 - f. Excessive use of district technologies for recreational, entertainment, or purely personal uses of email during the work day that may interfere with their ability to perform their job responsibilities.
 - g. Commercial purposes, such as offering, providing or purchasing products or services through the district's system.
 - h. Attempting to connect to district wireless access points without prior authorization.
 - i. Unauthorized use of electronic communication devices or personal digital assistants (PDAs) to gain advantage in the classroom.
 - j. Falsifying a user name or password in order to gain access to un-authorized areas of the district system.
9. Academic Freedom, Selection of Material, Student Rights to Free Speech
- a. Board policies on academic freedom and free speech will govern the use of the Internet.
 - b. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that are relevant to the course objectives. Teachers should make every attempt to preview the materials and sites they require or recommend student's access to determine the appropriateness of the material contained on or accessed through the site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.
10. District Web Site
- a. District Website – The district will establish a website and webpages that will present timely information about the district. The Instructional Technology Coordinator, or his/her appointee, will be responsible for maintaining the district Web site.
 - b. School and Classroom Class Websites – Schools and classrooms will establish websites that present timely information about the school and/or classroom activities and must be located on the district approved web host. The building Principal will designate an individual to be the school “webmaster” and person responsible for managing the school website. Teachers will be responsible for maintaining their classroom website.

- c. Extracurricular Organization Web Pages – With the approval of the building Principal, extracurricular organizations may establish Web pages. The Principal will establish a process and criteria for the establishment and posting of material, including links to other sites, on these pages. Material presented on the organization Web page must relate specifically to organization activities and must include the following notice: “This is a extracurricular organization webpage. Opinions expressed on this page shall not be attributed to the district.”
- d. District web pages shall comply with legal requirements regarding the use, reproduction, and distribution of copyrighted works. Therefore, no copyrighted information should be placed on the District web page except with the written permission from the creator of the work, or otherwise permitted by law. Official trademarks or logos also may NOT be placed on the District web page without receiving appropriate permission.
- e. The District retains all proprietary rights to the content of all pages on the district/individual school’s website, absent written agreement to the contrary.

11. Consequences

- a. Violation of these guidelines can result in restricted network access, loss of privileges, and disciplinary and/or legal action including, but not limited to, expulsion, and criminal prosecution under appropriate state and federal laws. Appeals may be made in accordance with appropriate Board policies, procedures, employee contracts and student handbooks.
- b. 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

Approved: September 27, 1997

Revised: July 27, 2009

Policy 6.28 Attachment(s) Acceptable Use Handbook Summary

The School District of Brown Deer telecommunication system provides student and staff access to the appropriate and standard equipment and online resources for use in curriculum activities and classroom projects. District telecommunication users are expected to exercise responsible behavior when using these resources and clearly realize that basic use is a PRIVILEGE and NOT A RIGHT. Responsible behavior includes, but is not limited to, the following:

- represent your school and yourself in a positive manner
- being courteous, polite and avoiding inappropriate language in all forms of communication
- keep personal information private; use only first names when online
- abide by all security restrictions; never attempting to evade or disable for unauthorized access
- properly maintaining all equipment; vandalism will not be tolerated
- remain on task; appropriately using the resources provided by the teacher

In addition, staff and students will adhere to the following guidelines:

Respect for System Security

- Users are responsible for the use of their individual network account and should take all reasonable precautions to prevent others from being able to use their account.
- Under no condition should a user provide their password to another person or attempt to access or use resources assigned to another user.
- Users will immediately notify a person in charge if they have identified a possible security problem.
- Users will not intentionally avoid or evade district security measures used to filter the Internet, track usage or maintain computer systems.
- Users will avoid the inadvertent or intentional spread of computer viruses by following established virus detection procedures.

Respect for Resource Limits

- Users will use the system only for educational and professional or career development activities.
- Downloading of files is prohibited, except by authorized staff.
- Users will not use their district network storage as place to maintain and house non-school related files (i.e. games, music, photos, video, etc.)
- Users will properly maintain all files and folders in order to stay within a established quota.

Respect for Privacy

- Users will not re-send or forward an e-mail message without first getting permission from the original sender of the message.
- Users will not post/send private, discriminatory, or defaming information about another person.

Specific Unacceptable Uses

- Users will not use the District system for commercial purposes, defined as offering or providing goods or purchasing services for personal use.
- Users will not attempt to gain unauthorized access to the district network or to any other computer system through the district network, or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files.
- Users will not use the district system to engage in any illegal or unethical acts which include but are not limited to:
 - posting information that could cause damage or a danger of disruption
 - posting false or defamatory information about a person or organization
 - plagiarizing works found on the Internet or copyright infringement
 - using the network to intimidate, humiliate, or threaten another individual
 - using the network to access materials that are inappropriate, pornographic, obscene, advocate violence or discriminate against others.

Consequences

Violation of these guidelines can result in restricted network access, loss of network privileges, and disciplinary and/or legal action including, but not limited to, expulsion or dismissal, and criminal prosecution under appropriate state and federal laws.

**Policy 6.28 Attachment(s)
Acceptable Use of the District Technology
Letter**

Date

Dear Parent(s) or Guardian(s):

This school year your son or daughter will have access to the School District of Brown Deer network which includes access to the Internet and various other online resources deemed appropriate by the teacher. The purpose of the network is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world. Student use of the Internet may include classroom activities, professional or career development, and limited high-quality self-discovery activities.

Elementary age students (preK-4th) may be given their own network login and passwords to access network resources. If an email account is needed, these students will be granted access only through a classroom account. Any time students are asked to identify themselves online they are to use **FIRST NAMES ONLY**. No other personal contact information (full name, address, telephone, personal email, age, etc) should be given at any time unless with full permission from parent/guardian.

Middle and high school age students (4th – 12th) will be given their own network login and passwords to access network resources including email service. Any time students are asked to identify themselves online they are to use **FIRST NAMES ONLY**. No other personal contact information (full name, address, telephone, personal email, age, etc) should be given at any time unless with full permission from parent/guardian if the student is a minor. A parent may request to have their child's network account terminated at any time by notifying the district in writing.

Safety on the Internet is a concern. The district network utilizes a sophisticated firewall to restrict access to inappropriate sites. Due to the nature of the Internet, no security system is fail proof. However, the School District of Brown Deer believes that the use of the firewall security system and teacher supervision of computer activities provides a safe, educational environment. Parents may request alternate activities for their children that do not require Internet access by notifying the district in writing.

Included with this letter is the Acceptable Use Handbook Summary listing the guidelines for use of the district network. Expectations for the appropriate use of technology include, but are not limited to, the conditions set forth in this agreement. Other expectations established by law, through school district policy, and/or established by each school must also be followed. Your child's access and use of the telecommunication network will be monitored by his/her teacher. Any questions about the use of the network can be directed to your child's classroom teacher or principal.

Respectfully,

Signed by Building Principal