STAFF/STUDENT TECHNOLOGY
INTERNET APPROPRIATE USE AND ONLINE SAFETY POLICIES

General Purpose

The School District of Chilton (District) recognizes the role of technology in preparing students for success in life and work in the 21st century. It also requires employees to learn to use the District's technology resources to perform tasks associated with their positions and assignments. To that end, the District will provide students and staff with appropriate access to its network, to the vast resources available through it, and to teacher instruction of a District-approved internet safety curriculum.

Staff, students, and School Board members must keep in mind that when they use the District network, their actions and communications may be identified as those of the District. As such, staff and Board members are to exercise professional judgment at all times when using the District's network and to conform to these policies.

The use of the District network and access to the Internet is a privilege, not a right. Users will be held responsible for their actions when using the network. Inappropriate uses will result in suspension or revocation of user privileges and/or other disciplinary action. User activity which is an apparent violation of law may be disclosed to law enforcement authorities or other third parties without prior consent of the offending person.

Demonstrated intent to violate this policy may be considered the same as an actual policy violation. Demonstrated intent means evidence of actions that, if successful or if carried out as intended, would result in a policy violation.

Limited Educational Purpose

The purpose of the District network is to support and enhance education in the School District of Chilton. Uses that might be acceptable on a personal account on another system may not be acceptable on the District educational system. Appropriate uses include instructional activities and assignments, as well as professional or career development activities.

No Expectation of Privacy

In view of the nature of the District network and its stated purpose, no user may expect that their communications or files will be private or remain confidential. Users should have no expectation of privacy or confidentiality in the content of any message or document created, archived, stored, retained, displayed, received, solicited, deleted, looked at, or sent with the District's resources. The District reserves the right to monitor, access, and/or disclose the content of any of these messages or files without prior notice to the user. The District also reserves the right to remove any files from the District network without prior notification.

CIPA and NCIPA

In accordance with requirements of the Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA), all equipment connecting to the Internet from any connection located within the District's buildings will be blocked or filtered. The District must take effective steps 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. The District will also take effective steps 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:

A. Pornographic or erotic images
B. Sexual implications
C. Racial slurs
D. Derogatory gender-specific comments
E. Information or instructions designed to cause harm to other person(s)/organization(s), comments that offensively address a person's age, sexual orientation, beliefs, political beliefs, gender, religious beliefs, national origin or disability

F. Any comment which in any way defames, slanders, or libels another person(s)

G. Any comment intended to frighten, intimidate, threaten, abuse, annoy, or harass another person(s), or organization(s)

H. Those data or activities that invade the privacy of another person(s)

In addition, the District will also take effective steps to prevent unauthorized access to its system and files, including so-called "hacking" and the unauthorized disclosure, use or dissemination of personal identification information regarding minors. To meet this requirement, the District will use software and staff to routinely monitor users' activities. The District acknowledges that no blocking or filtering mechanism is capable of stopping all inappropriate content all of the time. Therefore, students are not to use the District's Internet access without supervision by a staff member. The potential failure of a blocking or filtering mechanism to operate as intended does not excuse anyone, using the School District network, from conforming to this policy or authorize anyone to violate this policy.

It is the responsibility of the staff to guide and to monitor students in the effective and appropriate use of the District network. This includes, but is not limited to:

A. Teaching students how to find educationally appropriate electronic materials.

B. Teaching students how to judge the educational suitability of electronic materials.

C. Teaching students information literacy skills, including understanding of safety, copyright, and data privacy.

D. Teaching students proper safety and security procedures when using electronic mail, chat rooms, and other forms of direct electronic communication.

Management and Administration

All software loaded on District computers and servers must be properly licensed and documented. Any unlicensed or unauthorized software found on the District network will be removed.

Viruses can cause a significant disruption to the District network. Therefore, the District will, where possible, implement virus-scanning systems and processes to eliminate or significantly limit damage to its network from these programs.

All users must comply with federal, state, and local laws governing intellectual property, software licenses and copyrights. Copyrighted materials, including text, pictures, video, sound, and other attachments, should not be copied or distributed using the District computer resources without appropriate credit and, where necessary, permission from the author, composer, and/or owner, photographer, videographer and, where applicable, payment of license fees.

Internet Safety Education

Staff members will participate in professional development programs, as appropriate, in accordance with the provisions of this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social networking sites and other forms of electronic communications, including the proper use of and behavior in an online environment;

B. the inherent danger of students disclosing personally identifiable information online;

C. the use of netiquette to avoid cyber bullying and steps for dealing with the issue of a cyber bully;

D. the need for firewalls, virus and spyware blocking software; and,

E. the consequences of unauthorized access (e.g., "hacking"), cyber bullying and other unlawful or inappropriate activities by students or staff online.

In accordance with the Broadband Data Improvement Act (S.1492), staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above.

The disclosure of personally identifiable information about students online is prohibited.

Students may not access social media for personal use from the District network, but may be permitted limited access to social media for educational use in accordance with a teacher's approved plan.

Usage Guidelines

All use of the District network by students and staff, including Internet, must be consistent with the focused educational purpose stated in this policy. The School District cannot articulate all required or proscribed behaviors by users of the system. To assist however, the following general standards of conduct are prescribed:

Users are expected to abide by the generally accepted rules of network etiquette, which include, but are not limited to:

A. Be polite. Users are not to send or forward abusive messages or engage in cyber bullying.

B. Use appropriate language. Users are not to swear, use vulgarities, obscenities or any other language inappropriate in a school setting.

C. Do not use the network in a way that disrupts use by others.

D. Any user who finds him or herself connected to a site that is inappropriate must immediately disconnect from that site and then inform a teacher (student user) or supervisor (employee user) of the incident. Information about this site will be communicated to the Director of Technology.

E. All communications and information accessible via the network should be assumed to be copyrighted property, unless specifically identified otherwise.

F. All users shall:

1. Not share confidential information regarding students or employees.
2. Recognize that Internet usage is a privilege, not a right.
3. Recognize that there may be inappropriate exposure to obscene or objectionable material through their access to the Internet.
4. Not use the District network to access, review, display, upload, download, solicit, store, print, post, retain, or distribute pornographic, obscene, or sexually explicit material.
5. Not use the District network to transmit or receive obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language.
6. Not use the District network to access, review, display, upload, download, solicit, store, print, post, retain, or distribute materials that use language or images that are inappropriate in the educational setting or are inconsistent with the standards of the community or disruptive to the educational process.
7. Not intentionally waste limited resources.
8. Not use the District network to access, review, display, upload, download, solicit, store, print, post, retain, or distribute materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or cyber bullying.
9. Not use the District network to engage in any illegal act, including copyright infringement, or violate any local, state, or federal statute or law.
10. Not violate regulations prescribed by the network provider.
11. Not use the District network to gain unauthorized access to information resources or to access another person's materials, information, or files without the permission of that person.
12. Not tamper with, modify, disable or change the District network software, hardware, or wiring or take any action to violate the District system security, and not use the District system in such a way as to disrupt use of the system by other users.
13. Not use the system for mass distribution of commercial solicitations or unofficial fundraising messages.
14. Not post an anonymous message, forge or disguise a return address, or send a message through a "re-mailer."

15. Acknowledge that all computers, their attached equipment, peripherals and the software installed within these systems are the property of the School District of Chilton.
16. Acknowledge that the Internet and e-mail communications are public and not private in nature and that the District reserves the right to monitor and access every aspect of an individual's Internet activities and e-mail content.
17. Not plagiarize materials that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own. Students will abide by plagiarism rules and regulations concerning digital data and its use.
18. Not use the School District of Chilton network to access material that is profane or obscene (pornography) or that advocates illegal acts or violence or discrimination toward other people (hate literature). A special exception may be made for hate literature if the purpose of the access is to conduct research within an established curriculum, with both teacher and parental approval. In addition, students will not use the network to access information on how to make or use explosives, explosive devices, firearms, or other weapons.

G. All staff shall:

1. Keep student information confidential and not reveal information unless the release is authorized by law or consent, and the person(s) receiving the information is authorized access to the information by law or consent.
2. Conform to this policy and other rules on the use of the Internet and school technology systems. This is to include only use by a School District of Chilton employee, which requires the use of the login password and appropriate passwords. Unacceptable use includes use for personal business, commercial or financial gain, soliciting or lobbying for political or religious causes, use for unethical or disruptive activities, sending junk mail or chain letters, and becoming a member of non-work related list serves.
3. No School District e-mail or Internet system shall be used to send jokes or other comments that may be pornographic, discriminatory, harassing, or offensive to others, or material that defames an individual, company or business, or discloses personal information without authorization. Penalties may include criminal sanctions under Wis. Stat 947.0125 for threatening, abusive, frightening or intimidating messages sent to another person(s) through e-mail or other computerized communications systems including voicemail.
4. Adhere to the School District policy on sexual harassment that states employees are not to access pornographic sites or display images of a sexual nature on their monitors. This shall include child pornography and harmful images (nudity, torture, brutality) which may be viewed by students. This conduct is subject to potential criminal sanctions under 18 U.S.C. 2252 and Wis. Stats. Sections 948.11 and 948.12.
5. Abide by copyright restrictions, including the illegal copying or publication of material in digital format. Penalties may include personal liability when the employee violates copyright laws.
6. Not conduct union business except as specifically related to base wage negotiations and approved by the Superintendent of Schools.

H. All students shall:

1. Immediately disclose to his/her teacher any message s/he receives that s/he believes to be inappropriate or in violation of this policy.
2. Not use the District network to knowingly post unauthorized, false, or defamatory information about another person(s) or organization(s), or to harass another person(s), or to engage in personal attacks, including attacks which are discriminatory, based upon personal characteristics or a protected classification such as race, disability, and sexual orientation.
3. Not use the District system to vandalize, damage, or disable the property of another person(s) or organization(s).
4. Not attempt to or actually degrade, disable or disrupt equipment, software, or system performance by spreading computer viruses or by any other means.
5. Not attempt to log in through another person's account, or use computer accounts, access codes, or network identification other than those assigned to the user.

I. Non-Students/Non-Staff shall:

1. Acknowledge that the Internet and e-mail communications are public and not private in nature. The District reserves the right to monitor and access every aspect of any Internet activities engaged in.
2. Conform to this policy and all School District rules related to use of the Internet and school network including any use of computers or School District of Chilton systems. This includes NOT using the network for personal business purposes, soliciting or lobbying for political or religious causes, use for unethical or disruptive activities and sending junk mail or chain letters.
3. The system may be used for career advancement and educational research.
4. Immediately disclose to a staff member any message received which is believed to be inappropriate or in violation of this policy.
5. Not use the District network to access, review, display, upload, download, solicit, store, print, post, retain, or distribute pornographic, obscene, or sexually explicit material.
6. Not use the District network to transmit or receive obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language.
7. Not use the District network to access, review, display, upload, download, solicit, store, print, post, retain, or distribute materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment or discrimination.
8. Not use the District network to knowingly post unauthorized, false, or defamatory information about another person(s) or organization(s), or to harass another person(s), or to engage in personal attacks, including attacks which are discriminatory, based upon personal characteristics or a protected classification such as race, disability, and sexual orientation.
9. Not use the District network to vandalize, damage, or disable the property of another person or organization.
10. Not attempt to or actually degrade or disrupt equipment, software, or network performance by spreading computer viruses or by any other means.
11. Not use the District network to gain unauthorized access to information resources or to access another person's materials, information or files.

Because of the complexity and cost of technology, any user may be held personally responsible for the cost of repairing damage to or replacing computer resources, including but not limited to the replacement of equipment and/or payment for the time and materials required to repair the damage, when such damage is the result of a user's deliberate or negligent misuse of computer resources.

E-Mail Guidelines

A. E-mail is provided to enhance the work and academic performance of Chilton School District staff and students.

B. Access to e-mail is a privilege and not a right. The District may deny e-mail privileges in part or in the entirety at any time.

C. Students are only allowed to access their District provided e-mail accounts.

D. Electronic mail messages on District computers, networks, and facilities are District property and not personal property. There is no expectation of privacy or confidentiality provided and none should be assumed.

E. Electronic mail messages that contain inappropriate content or attachments (for example, remarks or images) are considered the same as if spoken or written in a document, and may result in consequences under existing rules concerning harassment (including, but not limited to: sexual, racial or bullying) or discrimination and/or other provisions relating to user conduct.

F. All e-mail messages are subject to request and disclosure under the Wisconsin Open Records Statute and should be considered official records.

G. The District maintains a central or distributed electronic mail archive of all electronic mail sent or received. The length of time these archives will be preserved is a matter within the discretion of the designated systems manager, subject to the Wisconsin Open Records Statute.

H. Staff and students are reminded of their obligation to respect intellectual property rights that may attach to materials that are included in e-mail—such as copyrighted images or text—and not to distribute copyrighted material electronically without the permission of the copyright owner.

I. It is prohibited to introduce classified information into an unclassified system. The use of "personal" encryption is prohibited.

J. Users are permitted limited personal use of the email system. Limited personal use means occasional individual messages that are not official use, that are of limited size, and that are otherwise in conformance with District policies and procedures. The Director of Technology will report to the Superintendent of Schools, personal use of the email system which contravenes this rule.

K. Abuse of e-mail privilege includes (but may not be limited to):

1. Use for unofficial purposes that interferes with the conduct of School District business or individual performance
2. High frequency or high volume messages
3. Sending e-mail messages or attachments of unreasonably large size
4. Sending messages that negatively impact the network performance or violate this policy

L. Use of the e-mail system should not reflect negatively on the School District. Users must be aware that concerns may be raised if their Chilton e-mail address is used in inappropriate venues. For example, providing input to a basketball discussion board or use group with any District provided e-mail address may raise the public's ire about District user conduct, regardless if the posting occurred during lunch or after normal business hours.

M. E-mail sent using a Chilton School District e-mail account must not be sent with the purpose or intent to defraud, intimidate, or otherwise commit an unlawful act.

N. Nothing intended to secure commercial gain from other District e-mail system users may be transmitted using the District e-mail system. Staff and students may not use the District e-mail system to transact any business activity that is of a for-profit nature.

Web Publishing Guidelines

Individuals creating web pages that will link to or be linked from the District's homepage will adhere to the following rules in order to provide consistency and integrity, but not to limit creativity.

A. The person that creates the web page that is linked to the District homepage is ultimately responsible for the web site content including links. The District has the right to approve the pages.

B. Web site links must be to sites that conform to District policies and be limited to educational material.

C. Names and photos of students may be used on the District website unless written permission denying approval is on file. Student photographs will be identified as an element of School District directory data in Board of Education policy and annual notices.

D. Web sites should clearly be identified as student or staff-created web pages and that student or staff opinions do not necessarily reflect the position of the District.

E. Web sites may not contain confidential information of any character, or information the disclosure of which, represents a violation of law or the policies of the Board.

F. Web sites may not contain copyrighted materials without proper permission.

Open Meetings and Public Record Law

In using the District's computer network, Board members shall comply with Wisconsin's Open Meetings and Public Records Laws. E-mail and computer transmissions among Board members may be "a gathering of members of a public body to conduct governmental business" and therefore a meeting requiring prior notice and compliance with the open meetings law. E-mail and other transmissions between Board members are required by law to be preserved and may be subject to disclosure.

Limitation on District Liability

The District is not responsible for the accuracy or quality of any advice or information acquired through or stored on the District network.

The District makes no guarantee that the functions or the services provided by or through the District network will be error-free or without defect. The District is not responsible for the accuracy or quality of the information acquired through or stored on the system.

The District shall not be responsible for financial obligations arising out of unauthorized use of the District's network or the Internet.

The District shall have no liability arising out of or related to nonavailability of data stored on school data systems, including but not limited to diskettes, tapes, hard drives or servers, or for delays or changes in or interruptions of service or miss-deliveries or non-deliveries of information or materials, regardless of the cause.

The District cannot and does not guarantee that all electronic materials accessed by students using the District network will be educationally appropriate, notwithstanding preventive steps taken.

The District cannot and does not guarantee that any electronic messages or communications sent or received by staff using the District network are or will remain confidential. Any message may become public knowledge through inadvertence, misuse of the network, application of the Wisconsin Open Records Law, or other reasons.

Penalties/Consequences

The District will cooperate fully with local, State, Federal or international officials in any investigation related to illegal activities involving use of the School District of Chilton has occurred, the person will be given notice of suspected violations and the violation, as well as the number of previous violations, consequences could include, but are not limited to, the following: immediate referral to administration; suspension or cancellation of access privileges; suspension or expulsion from school; payments for replacement, and penalties; referral to law enforcement officials; and/or discipline under other School District policies. Consequences for School District of Chilton employees include appropriate administrative discipline up to and including termination.

All staff members and students will sign a Computer and Internet Appropriate Use Agreement. A parent/guardian must also sign the Technology and Internet Appropriate Use Agreement consenting to each student's use of the Internet.

Adopted 5/16/05
Revised 8/27/12
Revised 10/22/12