

CHADWICK MILLEDGEVILLE CUSD 399

TECHNOLOGY USE POLICY

ACCESS TO TECHNOLOGY – Including Student Laptops, Networked Computers and the Internet

The School Board's goal is to include technology in the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication.

The School District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Individual School Board members, administrative staff and support staff members shall be considered as "teacher" with regard to this policy. "Internet" includes all information accessed by Internet sites, E-Mail, on-line services, and bulletin board systems.

CURRICULUM

The use of technology shall be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students. The technology shall comply with the selection criteria for instructional materials and library-media center materials. Teachers will use technology, including the Internet, throughout the curriculum. The Internet is part of the curriculum and is not a public forum for general use.

ACCEPTABLE USE

All use of the District's connection to technology, including the Internet, must be in support of education and/or research, and be in furtherance of the School Board's stated goal. Use is a privilege, not a right. General rules for behavior and communications apply when using the Internet. Appropriate uses, ethics, and protocol for the internet and student laptops are listed below. Electronic communications and downloaded material may be monitored or read by school officials.

AUTHORIZATION FOR TECHNOLOGY ACCESS

Each student and his or her parent(s)/guardian(s) must sign the *Student Laptop Agreement Form* before being granted unsupervised use of technology, including networked computers and the Internet.

The failure of any student to follow the terms of the *Student Laptop Home Agreement* or this policy will result in the loss of privileges, disciplinary action, and or appropriate legal action.

All use of technology shall be consistent with the district's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. The *Student Laptop Home Agreement* does not attempt to state all required or proscribed behavior by users, however, some specific examples are provided.

The failure of any user to follow the terms of the Authorization for Technology Access will result in the loss of privileges, disciplinary action, and/or appropriate legal action. Consequences may include the following steps:

1. Loss of school laptop take home privileges for 2 weeks + detention.
2. Loss of school laptop take home privileges for 4 weeks + detention or suspension.
3. Loss of school laptop take home privileges for remainder of school year.

The signature(s) at the end of this document is/are legally binding and indicate(s) the party who signed has read the terms and conditions carefully and understands their significance.

TERMS AND CONDITIONS

1. **Acceptable Use** – access to the District's technology must be for the purpose of education or research, and be consistent with educational objectives of the district, or for legitimate business use.

2. **Privileges** – The use of the District’s Technology is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The Superintendent, Principal, Director of Technology will make all decisions regarding whether a user has violated this *Authorization* and may deny, revoke, or suspend access at any time; his or her decision is final.
3. **Unacceptable Use** – You are responsible for your actions and activities involving the network. Some examples of unacceptable use are:
 - a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;
 - b. Using a non-authorized device (mp3 player, tablet, phone, personal laptop, etc);
 - c. Unauthorized downloading of software, regardless of whether it is copyrighted or virus free;
 - d. Downloading copyrighted material for personal use;
 - e. Using the network for private financial or commercial gain;
 - f. Wastefully using resources, such as file space;
 - g. Hacking or gaining unauthorized access to files, resources, or entities;
 - h. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature;
 - i. Using another user’s account or password;
 - j. Posting material authorized or created by another without his/her consent;
 - k. Posting anonymous messages;
 - l. Using the network for commercial or private advertising;
 - m. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material, or otherwise engaging in cyber-bullying. Cyber-bullying is defined as the use of the Internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner; and
 - n. Using the network while access privileges are suspended or revoked.
4. **Network Etiquette** – The user is expected to abide by generally accepted rules of network etiquette. These include, but are not limited to, the following:
 - a. Be polite. Do not become abusive in your message to others.
 - b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
 - c. Do not reveal personal information, including the addresses or telephone numbers of students or colleagues.
 - d. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
 - e. Do not use the network in any way that would disrupt its use by other users.
 - f. Consider all communications and information accessible via the network to be private property.
5. **No Warranties** – The district makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
6. **Indemnification** – The user agrees to indemnify the School District for fees, costs, or damages, including reasonable attorney fees incurred by the District, relating to, or arising out of, any breach of these procedures.
7. **Security** – Network security is a high priority. If the user can identify a security problem on the Internet, you must notify the system administrator or Building Principal. Do not demonstrate the problems to other users. Keep the user’s account and password confidential. Do not use another individual’s account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.
8. **Vandalism** – Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.
9. **Telephone Charges** – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per minute surcharges, and/or equipment or line costs.

- 10. Copyright Web Publishing Rules** – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Web sites or file servers without explicit written permission.
- a. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
 - b. Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of “public domain” documents must be provided.
 - c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.
 - d. The “fair use” rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
 - e. Student work may only be published if there is written permission from both the parent/guardian and student.

11. Use of Electronic Mail

- a. The District’s electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an educational tool.
- b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account’s user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
- c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.
- d. Electronic messages transmitted via the School District’s Internet gateway carry with them an identification of the user’s Internet “domain.” This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message’s authenticity and the nature of the file so transmitted.
- f. Use of the School District’s electronic mail system constitutes consent to these regulations.

12. Internet Safety

- a. Internet access is limited to only those “acceptable uses” as detailed in these procedures. Internet safety is almost assured if users will not engage in “unacceptable uses,” as detailed in these procedures, and otherwise follow these procedures.
- b. Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in these procedures.
- c. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children’s Internet Protection Act and as determined by the Superintendent or designee.
- d. The system administrator and Building Principals shall monitor student Internet access.