

Cache County School District

Policy Series 4000: Curriculum, Instruction, Assessment

Policy No. 4600 P1

Technology Acceptable Use

Definitions

“Electronic device(s)” means a device that is used for audio, video, or text communication or any other type of computer or computer-like instrument including:

- A. a smart phone;
- B. a smart or electronic watch;
- C. a tablet; or
- D. a virtual reality device.

“Inappropriate matter” means pornographic or indecent material as defined in Subsection 76-10-1235(1)(a) and Section 53G-10-103.

“District owned device(s)” means a device that is used for audio, video, text communication, or other type of computer or computer-like instrument that is identified as being owned, provided, issued, or lent by the district or individual school to a student or employee.

“Privately owned” means a device, including an electronic device that is used for audio, video, text communication, or other type of computer or computer-like instrument, that is not owned or issued by the district or individual school.

“The Children’s Internet Protection Act or CIPA” means federal regulations enacted by the Federal Communications Commission (FCC and administered by the Schools and Libraries Division of the FCC.

Filtering and Monitoring

- A. Filtering software is used on the district network to block or filter access to objectionable material in accordance with the Children's Internet Protection Act (CIPA).
- B. Staff must be aware that students have access to the Internet from all of the district’s computers. Despite the use of district filtering software, it is impossible to block access to all objectionable material. Teachers must use good judgment and closely supervise their students’ use of the Internet. On occasion, users of online systems may encounter material that is controversial and which other users, parents, or staff may consider inappropriate or offensive. Students or staff should notify the appropriate school authority if dangerous or inappropriate information or messages are encountered. Every user must

take responsibility for his or her use of the network and Internet and avoid objectionable sites or materials.

- C. Any efforts to bypass the district's internet and email filters or hide inappropriate online activity are prohibited. This includes, but is not limited to, using proxies, special ports, altering browser settings, or employing any other methods aimed at evading filters or accessing or sharing inappropriate matter.

Copyright and Trademarks

- A. Staff and students are required to respect the copyright laws and the rights of copyright owners. Copyright law information has been provided to each school library media center for reference. Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials, without the specific written permission of the copyright owner, is generally prohibited.
- B. The Fair Use Doctrine of the United States Copyright Law (Title 17, USC) allows for the duplication and distribution of materials for educational purposes within the four walls of a classroom and when content is cited appropriately. Once those materials leave the four walls of that room, such as a podcast or video placed on a website, fair use ceases to apply, and all copyright laws are in full effect.
- C. An individual may be breaking the law if he/she reproduces or uses a work created by someone else without permission. Whenever a user is unsure about using a copyrighted work, obtain permission first from the copyright owner.
- D. Trademarks, such as logos and names representing a company, are protected under trademark law. Permission should be obtained prior to using trademarked names in any widespread publications, such as on the web.

Student Directory Information

- A. Cache County School District may disclose appropriately designated "directory information" without written parental consent, unless the parent has advised the district otherwise. An opportunity to opt out of disclosure is provided as part of the registration process.
- B. The primary purpose of directory information is to allow the district to include this type of information in certain school publications. Examples include:
 - a. a playbill, showing the student's role in a drama production;
 - b. the annual yearbook;
 - c. honor roll or other recognition lists;
 - d. graduation programs; and
 - e. sports activity sheets, such as for wrestling, showing weight and height of team members.
- C. To support activities such as publishing yearbooks or facilitating admissions at institutions of higher education, designated directory information may be shared with

outside organizations. This sharing will occur without prior written consent for these relevant purposes. In addition, two federal laws require local educational agencies (LEAs), receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA), to provide military recruiters, upon request, with names, addresses and telephone listings. This information could include:

- a. student first and last name;
- b. student gender;
- c. student home address;
- d. student photograph;
- e. student dates of attendance (years);
- f. student grade level;
- g. student diplomas, honors, awards received;
- h. student participation in school activities or school sports;
- i. student weight and height for members of school athletic teams; and
- j. student's most recent school attended.

No Expectation of Privacy

- A. No user should have an expectation of privacy when using the district network or district owned devices or equipment.
- B. The district reserves the right to disclose, to law enforcement officials or third parties, any electronic messages, as required for a legally justified investigation. These messages could include:
 - a. any email, chat, or other electronic communication using the districts supplied services; or
 - b. any electronic communications on district owned devices.
- C. All documents used on school computers are subject to public records disclosure laws.
- D. Any privately owned electronic device installed or connected to the district network, and all information and data on it, is subject to the policies of the school board and any additional school or district department guidelines.
- E. Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. The district reserves the right to monitor, inspect, copy, review and store information without prior notice.

Use of District Owned Devices

- A. The school district provides a variety of devices to both students and staff to facilitate teaching and learning and to help employees to conduct the business of the district. Many of these devices are mobile to allow staff flexibility and movement in order to accomplish their work.
- B. There is an expectation that mobile devices will be used primarily for purposes related to the business of the district. However, there is also an

understanding that these devices can be important to both personal and business productivity. For example, employees may keep calendar items or to-do lists for both personal and business purposes. This is appropriate and expected. A good rule to follow is that all

district owned devices should be used primarily for business purposes.

- C. District owned mobile devices should be tagged in accordance with the Business Office's inventory and tracking procedures. During asset audits, these devices should be available for inspection to ensure they are tagged and tracked properly. School inventories should indicate the primary location of the device and person responsible for the device.
- D. The use of district owned devices to access inappropriate matter, whether on or off district property, is prohibited and may result in criminal, employment, or student disciplinary consequences. If appropriate, this may be reported to law enforcement.

Use of Privately Owned Devices

- A. All use of the district network and Internet system on privately owned cell phones or other digital devices while on-campus is subject to the district's Student Cellular Device Policy. Users may not share or post personal information about or images of any other student or employee without permission from that student or employee.
- B. If a user is found to have abused a privately owned cell phone or digital device in a manner that is not in accordance with this policy or the district's Student Cellular Device Policy, the administrator may ban the user's use of any and all privately owned electronic devices on the district network.
- C. An educator who allows the use of privately owned electronic devices, including cellular phones, in the classroom must:
 - a. ensure that usage is in accordance with this policy and the Student Cellular Device Policy; and
 - b. clearly communicate to parents and students the conditions under which the use of a privately owned electronic device is allowed.
- D. The use of privately owned devices on school property or at school-sponsored events to access inappropriate matter, whether on district networks or personal data connections, may have criminal, employment, or student disciplinary consequences, and if appropriate, may be reported to law enforcement.
- E. Privately owned electronic devices may use the district guest networks and internet system at the discretion of school administration, and connectivity may be restricted or terminated without notice at any time.
- F. Privately owned electronic devices shall only use designated guest networks, including eduroam, that are appropriately segmented from secure internal resources.
- G. Privately owned electronic devices shall, under no circumstances, be connected to the district's wired network and Internet systems.

Off-Campus Internet Expression

- A. Users may be disciplined for expression on off-campus networks or websites if the expression is deemed to cause a substantial disruption in school, or collide or interfere with the rights of other students or employees.
- B. Maintaining or posting material to a website or blog that threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other users to participate fully in school or extracurricular activities, can subject the student or employee to penalties and disciplinary action.

Warranties

- A. The Cache County School Board makes no warranties of any kind, whether expressed or implied, for the services provided.
- B. The School Board is not responsible for any damages suffered, including loss of data, in conjunction with the use of its networks or equipment.

Acceptable Use

Prohibited conduct includes, but is not limited to, the following:

- A. accessing, sending, creating, or posting materials or communications that are:
 - a. damaging to another person's reputation;
 - b. abusive;
 - c. obscene;
 - d. sexually oriented;
 - e. threatening or demeaning to another person;
 - f. contrary to the district's Bullying, Cyberbullying, Hazing, and Retaliation policy, whether with district or privately owned devices;
 - g. illegal; or
 - h. significantly impairing academic excellence.
- B. using the network for financial gain or advertising;
- C. posting or plagiarizing work created by another person without his/her consent;
- D. attempting to read, alter, delete, or copy the email messages of other system users;
- E. giving out personal information such as driver's license or social security numbers, bankcard or checking account information;
- F. using the school's computer hardware or network for any illegal activity;
- G. downloading, installing, or using games, music files, public domain, shareware or any other unauthorized program on any school's computer or computer system. Accessing entertainment sites, such as social networking sites or gaming sites, except for legitimate educational purposes under the supervision of a teacher or other professional;
- H. purposely bringing on premises, or infecting any school computer or network with, a virus, or program designed to damage, alter, destroy or provide access to unauthorized data;

- I. gaining access or attempting to access unauthorized or restricted network resources, or the data and documents of another person, including any other so-called “hacking” activities;
- J. using or attempting to use the password or account of another person, or utilizing a computer while logged on under another user's account. Providing another user with user account information or passwords;
- K. using the school's computers or network while access privileges have been suspended;
- L. altering or attempting to alter the standard configuration of a computer, network electronics, the operating system, or any of the software;
- M. attempting to vandalize any network or computer component;
- N. attempting to disconnect or disassemble any network or computer component without technology department oversight and authorization;
- O. connecting to or installing any computer hardware, components, or installing software on school devices without prior approval of the district technology personnel; or
- P. bypassing or attempting to circumvent network security, virus protection, or filtering.

Disciplinary Actions

- A. If a user violates any of the preceding policy provisions, his/her access may be limited or terminated and future access may be denied. In addition, appropriate disciplinary action may be taken, which may include, but are not limited to probation, termination, suspension, expulsion, legal action, and/or referral to law enforcement as appropriate.

Training

- A. Staff training shall be provided within the first 45 days of each school year covering the following:
 - a. the Technology Acceptable Use Policy including discipline related consequences due to policy violation (USBE Administrative Rule R277-495-5).
- B. Training will be provided utilizing the district’s supported training platform.

Student and Parent Acceptance

- A. Annually, within 45 days of each school year, a form containing the Technology Acceptable Use Policy will be included, along with the Bullying, Cyberbullying, Hazing and Retaliation Policy, in the district’s student information system, requiring parent and student acceptance.

Reporting

- A. Reports of misuse of electronic devices should be referred to school administration and the Director of Technology.
- B. The school administrator, to whom a complaint of inappropriate technology use is reported, shall promptly investigate the complaint. All acts of inappropriate technology

use that constitute criminal activity will be reported to law enforcement, who will assist with the investigation.

Exceptions

School administration may permit exceptions to this policy and procedures for health-related reasons or emergencies. These exceptions may include:

- A. diabetic monitoring devices; or
- B. use of privately owned cellular devices required for monitoring medical equipment.