Cache County School District's Acceptable Use Policy

Introduction

The Cache County School Board considers technology an essential tool in the educational process. There is an expectation that staff and students will use technology responsibly. To help promote good digital citizenship, the Cache County School District has adopted the following policies and procedures:

I. 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. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution by themselves. Filtering software is never 100% effective. On a global network such as the Internet, it is impossible to effectively filter everything. 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 attempts to subvert the District's Internet and/or e-mail filter or to conceal inappropriate Internet activity are prohibited, such as proxies, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the access or publication of inappropriate content.

II. Copyright & Trademarks

A. Board policy requires that students 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 – e.g.: in 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 you are 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.

III. 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 to the contrary. 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:

1. A playbill, showing the student's role in a drama production
2. The annual yearbook
3. Honor roll or other recognition lists
4. Graduation programs
5. Sports activity sheets, such as for wrestling, showing weight and height of team members.

C. Directory information can also be disclosed to outside organizations without prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings, or publish yearbooks, or institutions of higher education. 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 the following information – names, addresses and telephone listings. This information could include:

1. Student first and last name
2. Student gender
3. Student home address
4. Student photograph
5. Student dates of attendance (years)
6. Student grade level
7. Student diplomas, honors, awards received
8. Student participation in school activities or school sports
9. Student weight and height for members of school athletic teams
10. Student most recent school attended

IV. No Expectation of Privacy

A. No user should have an expectation of privacy when using the CCSD network or equipment.
B. The District reserves the right to disclose to law enforcement officials or third parties any electronic messages, as appropriate.
C. All documents used on school computers are subject to public records disclosure laws.
D. Any personal 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.

V. 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 that allow staff flexibility and movement of the assets 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 for both personal and business purposes, or to do lists for both personal or business use. 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.

VI. Use of Personal Devices

A. All use of the District network and Internet system on personal cell phones or other digital devices while on-campus is subject to the provisions of the individual school policies. Users may not share or post personal information about or images of any other student, staff member or employee without permission from that student, staff member or employee.
B. If a user is found to have abused a personal cell phone or digital device in a manner that is not in accord with this policy, the administrator may ban the user's use of any and all personal cell phone or digital devices on the district network.

VII. 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, staff 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.

VIII. 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.

IX. Acceptable Use

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

A. Accessing, sending, creating or posting materials or communications that are:
    1. Damaging to another person's reputation
    2. Abusive
    3. Obscene
    4. Sexually oriented
    5. Threatening or demeaning to another person
    6. Contrary to the school's policy on harassment or bullying
    7. Illegal
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.
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, disconnect or disassemble any network or computer component.
N. Connecting to or installing any computer hardware, components, or installing software on school devices without prior approval of the District technology personnel.
O. Bypassing or attempting to circumvent network security, virus protection, or filtering.

X. 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.