Fentress County Board of Education

Monitoring:	Descriptor Term:	Descriptor Code:	Issued Date:
	Fentress County Acceptable Use Policy	**4.4061**	**06-04-18 Revised**
		Rescinds:	Issued:

Updated April 30, 2018

The board provides its students and staff access to a variety of technological resources, including laptop computers and tablets. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. Through the school district's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

The board intends that students and employees benefit from these resources while remaining within the bounds of safe, legal, and responsible use. Accordingly, the board establishes this policy to govern student and employee use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

A. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

School district technological resources may only be used by students, staff and others expressly authorized by the Technology Department. The use of school district technological resources, including access to the Internet, is a privilege, not a right.

Individual users of the school district's technological resources are responsible for their behavior and communications when using those resources. Responsible use of school district technological resources is use that is ethical, respectful, academically honest, and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette. General student and employee behavior standards, including those prescribed in applicable board policies, the Student Code of Conduct and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school district computers or electronic devices or who accesses the school network or the Internet using school district resources must comply with the additional rules for responsible use listed in Section B, below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive. Furthermore, all students must adhere to the FCS Technology Use Guidelines as set forth in the Student Code of Conduct. Prior to using the Internet, all students must be trained about appropriate on-line behavior as provided in policy 4.406 Use of the Internet.

All students and employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using school district technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful

misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School district technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching. Use of school district technological resources for political purposes, sectarian religious purposes, or for commercial gain or profit is prohibited. Student personal use of school district technological resources for amusement or entertainment is also prohibited. Because some incidental and occasional personal use by employees is inevitable, the board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school district business and is not otherwise prohibited by board policy or procedure.

2. School district technological resources are installed and maintained by members of the Instructional Technology Department. Students and employees shall not attempt to perform any installation or maintenance without the permission of the Instructional Technology Department.

3. Under no circumstance may software purchased by the school district be copied for personal use.

4. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism.

5. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors. All users must comply with policy 5.500 – Discrimination/Harassment of Employees (sexual, Racial, Ethnic, Religious) and 6.304 Student Discrimination/Harassment and Bullying/Intimidation when using school district technology.

6. The use of anonymous proxies to circumvent content filtering is prohibited.

7. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.

8. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

9. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personal identifying information, or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves, fellow students, or any other person. For further information regarding what constitutes personal identifying information, see policy 4.406 Use of the Internet.

In addition, school employees must not disclose on school district websites or web pages or elsewhere on the Internet any private or confidential information concerning students, except as permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 6.600 Student Records. Users also may not forward or post personal communications without the author's prior consent.

10. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school district technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.

11. Users may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network without the express permission of the technology director or designee. Users enrolled in classes that teach game design or theory may follow the curriculum of their respective courses to create games. Users enrolled in computer classes teaching network design or maintenance may, with the assistance of their instructor, create programs as required by the course curriculum.

12. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.

13. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official. Students should log off or reboot at least once per day.

14. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.

15. Employees shall not use passwords or user IDs for any data system for an unauthorized or improper purpose.

16. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.

17. Teachers shall make reasonable efforts to supervise students' use of the Internet during instructional time, to ensure that such use is appropriate for the student's age and the circumstances and purpose of the use.

18. Views may be expressed on the Internet or other technological resources as representing the view of the school district or part of the school district only with prior approval by the superintendent or designee.

19. Without permission from the technology department, users may not connect any personal technologies such as laptops and workstations, wireless access points and routers, etc. to a district owned and maintained local, wide or metro area network. Connection of

personal devices such as iPods, iPads, smartphones, PDAs, and printers is permitted but not supported by technology department. Student teachers and other district invited guests are allowed to use the wireless access in support of their work inside Fentress County Schools. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service). While the technology department will make every reasonable effort to support personal devices, the district cannot guarantee a student or staff member will be able to access the network with a personally owned device.

20. District IT staff will assist any user with synchronization issues.

21. Those who use district owned and maintained technologies to access the Internet at home are responsible for both the cost and configuration of such use.

22. Employees and students who are issued district owned and maintained equipment must also follow these guidelines. All district employees and students are expected to follow these guidelines on all equipment owned by the District:

    a. Keep the equipment secure and damage free.

    b. Use the provided protective case at all times.

    c. Do not loan out the equipment, charger or cords.

    d. Do not leave the equipment in your vehicle.

    e. Do not leave the equipment unattended.

    f. Do not eat or drink while using the equipment or have food or drinks in close proximity to the equipment.

    g. Do not allow pets near the equipment.

    h. Do not place the equipment on the floor or on a sitting area such as a chair or couch.

    i. Do not leave the equipment near table or desk edges.

    j. Do not stack objects on top of the equipment.

    k. Do not leave the equipment outside.

    l. Do not use the equipment near water such as a pool.

    m. Back up data and other important files regularly. Fentress County Schools will at times perform maintenance on the equipment by imaging. All files not backed up to server storage space or other storage devices will be deleted during this process.

n. Do not check the equipment as luggage at the airport. It is usually advisable to carry any district owned equipment on board with you rather than checking it as luggage.

C. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The board recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless, school district personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that technology protection measures are used as provided in policy 4.406, Use of Internet, and are disabled or minimized only when permitted by law and board policy. The board is not responsible for content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service).

D. PARENTAL CONSENT

The board recognizes that parents and/or guardians of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent and/or guardian must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent/guardian and student must consent to the student's independent access to the Internet and to monitoring of the student's e-mail communication by school personnel.

In addition, in accordance with the board's goals and visions for technology, students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals. Parental and/or guardians permission will be obtained when necessary (i.e. when parental consent is needed by a site for CIPA laws) to create and manage such third party accounts.

E. PRIVACY

No right of privacy exists in the use of technological resources. Users should not assume that files or communications accessed, downloaded, created or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private. School district administrators or individuals designated by the superintendent may review files, monitor all communication and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer.

Under certain circumstances, the board may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the board, as a response to a public records request or as evidence of illegal activity in a criminal investigation.

F. SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Employees are responsible for reporting information security violations to appropriate personnel. Employees should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the board's network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a

security risk or having a history of problems with other systems may be denied access.

Users of school district technology resources are expected to respect school district property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school district is responsible for any routine maintenance or standard repairs to school system computers.

G. PERSONAL WEBSITES

The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school district or individual school names, logos or trademarks without permission.

1. Students

Though school personnel generally do not monitor students' Internet activity conducted on non-school district devices during non-school hours, when the student's on-line behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy.

2. Employees

Employees' personal websites are subject to policy 4.4.6, Employee Use of Social Media.

3. Volunteers

Volunteers are to maintain an appropriate relationship with students at all times. Volunteers are encouraged to block students from viewing personal information on volunteer personal websites or on-line networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. An individual volunteer's relationship with the school district may be terminated if the volunteer engages in inappropriate online interaction with students.

H. CYBERBULLING

1. Cyberbullying (using social media or any other Internet resource to do any of the things listed in following sentences) will not be tolerated. Harassing, disrespectful comments, or comments which could be reasonably construed to incite an argument or are intended to belittle another person, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

2. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

I. USAGE OF STUDENT IMAGES (PHOTOS AND/OR VIDEOS)

1. Fentress County Schools encourages students to become active participants in their education. As a result, we may publish photos and/or videos of students on web resources controlled by the district, as well as print media such as district publications and programs. **It is the parent/guardian's responsibility to notify the school in writing if they do NOT want their child's**

image or video posted.

2. **Note:** the *only* way to opt out of the district using the student's image is to provide *written* notification to the principal at your child's school that you do *not* give consent for images and/or videos of your child to be used in district resources and print media. Please be aware that teachers' ***professional*** social media accounts are considered "district resources" for the purpose of this AUP.

J. DISTRICT PROVIDED EMAIL ACCOUNTS AND ONLINE STORAGE

1. The Fentress County Schools has partnered with Google to provide email accounts and online file storage for everyone. This service is in full compliance with the provisions of The Children's Online Privacy Protection Act (COPA). COPA applies to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. No personally identifiable information is revealed to users outside the Fentress County Schools. Student usage and disclosure of personally identifiable information is covered in other sections of this document.

2. Email provided to students by the Fentress County Schools is filtered, monitored, and archived. District personnel are able to see all messages sent to or from any student account, but will not examine messages unless directed to by a competent authority (Principal, Director of Schools, or Law Enforcement with proper documentation).

K. PROFESSIONAL USE OF SOCIAL MEDIA

1. Fentress County Schools' employees should treat professional social media and communication like a professional workplace. The same standards expected in FCS professional settings are expected on professional social media sites.
2. All professional social media accounts will be associated with district provided and/or managed login credentials and privacy settings.
3. Users that establish a username and password for any FCS approved social media/online subscription for use by a school or classroom shall provide their username and password to building administration and administer the resource as any other professional social media.
4. All social media tools must be vetted by the district prior to use by a FCS employee and/or student.
5. Employees using professional social media have no expectation of privacy with regard to their use of social media.
6. Employees are responsible for protecting confidential information. No personally identifiable student information may be posted on professional social media sites, including student photographs, without consent of the students' parents/guardians.
7. Employees have an individual responsibility to understand the rules of the social media being used and act to ensure the safety of students. Employees are responsible for reporting use of social media not adhering to this agreement to building administration.
8. Employees are expected to use the TAP principle (Transparent, Accessible, Professional) in all social media usage.

L. PERSONAL USE OF SOCIAL MEDIA

1. The district recognizes that during non-work hours employees and students may participate in online social media, employees should keep in mind that information

produced, shared and retrieved by them may be subject to district policies and is a reflection of the school community. Policy 5.610

2. The personal social media presence should utilize the employee's personal emaiL address and should be completely separate from any professional social media presence.
3. Employees should not use their FCS email address for personal social media accounts.
4. FCS employees is discouraged from communicating with students who are currently enrolled in FCS schools on personal social media sites with the exception of a relative. If employees receive a request from a current FCS student to connect or communicate through a personal social media site, they are discouraged from accepting the request.
5. Employees should not tag other district employees, district volunteers, vendors or contractors without prior permission of the individuals being tagged.
6. Employees should not use the district nor school logo in any posting and should not conduct school business on personal sites without written permission from Fentress County Schools.
7. Personal social media use has the potential to result in disruption in the workplace and can be in violation of district policy and law. In this event, administration may have an obligation to respond and take appropriate action, including but not limited to investigation and possible discipline.
8. Employees should not access their personal social media accounts during the workday.
9. We encourage Fentress County Schools' employees to create a professional ONLY social media account, separate from personal, to post any school related material.

M. DISCLAIMER

The board makes no warranties of any kind, whether express or implied, for the service it is providing. The board will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries or service interruptions, whether caused by the school district's or the user's negligence, errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The school district specifically disclaims any responsibility for the accuracy or quality of information obtained through its Internet services.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-325(e)