Book	Procedures
Section	J: Students
Title	Acceptable Use of Technological Resources for Students
Number	JIK
Status	Under Review
Legal	Children's Internet Protection Act
Adopted	July 13, 1999
Last Revised	June 10, 2015
Last Reviewed	June 10, 2015
Origin	Formerly 347.35; adopted 7/13/99; revised 6/1/14, 6/10/15

Cross Reference: JIK Policy

A.   PURPOSE

The Garrett County Board of Education supports safe and appropriate use of the Garrett County Public School network infrastructure, internet, and equipment by students. This policy complies with the Children's Internet Protection Act [Pub L. No. 106-554 and 47 USC 254(h)].

The Garrett County Board of Education directs the administration to develop procedures that provide direction for acceptable use of technology by students.

B.   BACKGROUND

Garrett County Public Schools (GCPS) provides information technology equipment, services, and network access for educational purposes. These services are provided to improve learning and teaching through research, teacher training, administrative supports, collaboration, dissemination, and use of materials and resources. In addition, GCPS users (students, teachers, administrators, visitors) have no expectation of privacy while accessing email, the internet, or network resources while on GCPS' network. Access to networks both inside and outside of GCPS carries with it the responsibility for proper use of those resources and GCPS computing facilities. GCPS recognizes the fact that most computer users are responsible, thoughtful users. However, the actions of irresponsible users can disrupt and interfere with the rights of all users and will be subject to disciplinary action.

C.   DEFINITIONS

Educational purposes are defined in this regulation as those purposes directly related to a GCPS assignment, project, job, or function for which the user is responsible.

1.   Internet
       The name given to the collective public network of electronic devices and computer networks connected via the standard Internet protocol suite (TCP/IP).
2.   Intranet
       A private network inside a company or organization.
3.   Network
       The means of transmitting data between systems; includes wired and wireless technologies.
4.   Spam

Unauthorized and/or unsolicited electronic mass distribution (email/posts/etc.).

5.   Technology
     Electronic devices, network infrastructure, or any applications including but not limited to software, online resources, social media, and email.
6.   Web 2.0
     A term used to describe a new generation of Web services and applications with an increasing emphasis on human collaboration.
7.   Hacking
     Any unauthorized alteration of operating systems, individual accounts, software, networking facilities, teacher grade book and/or other programs.
8.   Jailbreaking or Rooting
     A device hack that removes limitations of a mobile device, allowing for software and hardware exploits.

D.   PROCEDURES

1. GCPS-owned technology equipment must be located and maintained in a safe, secure physical environment to protect against theft and/or damage. Users may be liable for costs as a result of thefts or damages in certain cases. All GCPS owned mobile devices that leave school property are required to be enrolled in the school system's MDM (mobile device management) program and linked to a specific person (employee or student). The purpose is to allow GCPS to easily track the whereabouts of its electronic devices.
2. Users are often allowed to access data on other networks and the computer systems attached to those networks. Each network or system has its own set of rules. Actions that are routinely allowed on one network or system may be controlled, or even forbidden, on other networks. It is the responsibility of the user to abide by the rules of every network or system.
3. Computer and network use is considered a privilege and inappropriate network use may result in termination of network privileges, disciplinary actions, and/or other actions determined appropriate, including legal action.
4. GCPS is not responsible for information found on networks outside of the GCPS organization, and GCPS does not have control over information residing on other systems to which there is access through GCPS. Some systems outside of GCPS may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.
     a. GCPS does not condone the use of or access to such information.
     b. GCPS cannot completely eliminate access to information that is offensive or illegal and residing on networks outside of the GCPS organization.
     c. GCPS limits access to objectionable material and visual objects that are obscene, pornographic or harmful to minors. It forbids the importation or possession of such information or material on any computer or network within GCPS. Procedures for disabling or modifying technology protection measures shall be the responsibility of the Director of [DotCom] Information Technology. Users are responsible for their actions when accessing information on networks.
     d. GCPS does not warrant network functionality or accuracy of information and is not responsible for information that may be lost due to system interruptions.
5. Users are expected to keep their disk storage space at an acceptable level. Unnecessary files should be removed on a regular basis.
     a. System administrators reserve the right to set quotas for disk usage on the system and to remove files if the user fails to maintain their storage area properly.
     b. System administrators reserve the right to supervise, monitor online activities of all users, and modify the network hardware, software and communications.
6. Users are responsible for their own individual accounts. Any violations that can be traced to account name will be treated as the sole responsibility of the account owner.
7. Personal Devices are permitted for instructional use only
     a. The student is personally responsible for any and all of their personal devices. The school shall not pay for, or reimburse any costs related to personal devices.
     b. The student assumes full liability for risks including, but not limited to, the partial or complete loss of school and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
     c. Students may not use camera devices on school property without permission from staff.
     d. Rooted, Jailbroken, or otherwise hacked devices are not permitted.
     e. Personal devices must be connected to the GCPS network – The use of cellular data on personal devices is forbidden.
     f. GCPS reserves the right to disconnected, or disabled services without notification.

8. It is impossible to document all appropriate conduct and use of computer facilities. To help users determine appropriate use and conduct, the following guidelines are provided. They are not   intended to be all inclusive, but should serve as a guide for appropriate use of computer facilities and network resources.

The following are examples of network use infractions that are prohibited:

1. Excessive use of the system for purposes other than education.
2. System tampering or "hacking"
3. Using obscene, vulgar, abusive or inappropriate language, pictures, or other material
4. Knowingly introducing viruses
5. Vandalizing, including equipment damage and willful tampering with data or software
6. Attempting to read, delete, copy or modify the electronic mail of other users
7. Attempting to decrypt passwords
8. Attempting to gain an unauthorized higher level of network privilege and access
9. Attempting to gain unauthorized access to remote systems
10. Deliberately interfering with other users
11. Making statements or taking actions that are libelous, slanderous, or constitute cyberbullying, harassment and intimidation of others
12. Permitting others to use your GCPS e-mail address, account, or password
13. Sharing passwords
14. Forging or attempting to forge e-mail messages
15. Unauthorized copying or transferring copyrighted materials or any other violation of copyright law
16. Placing copyrighted material on the network without the permission of the author
17. Plagiarizing, which is the taking of someone else's words, ideas, or findings and intentionally presenting them as your own without properly giving credit to the source
18. Using networks for illegal activities
19. Using commercial advertising, chain letters, or non-educational games
20. Altering, removing, or copying any computer application or software settings found in the operating system or application software provided by GCPS
21. Removing, defacing, or altering any identifying tags or markings on any computer or peripheral device
22. Using a private email account or other messaging system from any device on GCPS property for purposes not related to the educational program.
23. Be in possession of, download from the internet, install or use from any source: Software applications, browser plugins, operating systems, extensions, scripts, utilities or any other program code without authorization [The possession or use of a privately owned devices capable of transmitting, receiving or broadcasting, voice, data, video or music on GCPS property without authorization.]

E.   CONSEQUENCES OF UNACCEPTABLE USE

The smooth operation of the network relies upon the proper conduct of its users. The use of the Garrett County Schools' network infrastructure is a privilege, not a right. Should a student be found to have used the infrastructure inappropriately, her/his privileges may be revoked and future access may be denied. The misuse of the infrastructure may result in legal action as required by law.

Application for Garrett County Public Schools Internet Access - Student Form