

CHAPTER 8.00 - AUXILIARY SERVICES

TECHNOLOGY USE

8.331

These guidelines are based on the *Children's Internet Protection Act* (CIPA) and its four guiding principles of: respect, privacy, sharing, and safety. The Columbia County School District uses content filtering technology in compliance with CIPA on all computers and digital devices to protect against unacceptable web content. This Acceptable Use Policy is written for all those who use the Columbia County School District's provided "Network" connections and equipment. Electronic resources include, but are not limited to all hardware, software, data, communication devices, printers, servers, hubs, routers, switches, filtered Internet access, and local and wide area networks. All electronic equipment provided should be used in a responsible, efficient, ethical and legal manner.

- (1) General Policy and Guidelines.
 - (a) Inappropriate use of the Internet by students or school district employees may result in disciplinary action and/or cancellation of users privileges.
- (2) Use of Internet, Wide Area Network, Local Area Networks, Computers, Social Media Sites and Related Technology:
 - (a) All use of a network must be in connection with education and research and be consistent with the educational purposes of the Columbia County School District. It is expected that integration of the curriculum will be used with technology, as well as, students being given guidance and instruction in the use of technology. Teachers' supervision and monitoring is required to maintain effective and safe use of these resources.
 - (b) Students and staff shall not use the school district's computer network to solicit sales or conduct business. Students and staff shall not set up web pages for any reason without prior approval by a school administrator.
 - (c) Any use of a network for private or personal gain is prohibited.
 - (d) Any use of a network for product advertisement or political lobbying is prohibited.
 - (e) Users shall not intentionally seek information or obtain copies of data or passwords or modify files belonging to other users or misrepresent other users on the network. Identifications and

CHAPTER 8.00 - AUXILIARY SERVICES

passwords are confidential. If users give their identification or password to others (student or employees), they may lose their right to use the system. Example of identifying information include student's last name, home address and phone number. Students may be identified by their first names.

- (f) Students and staff should have no expectation of privacy or confidentiality in the content of electronic communications or other computers files sent and received on the school computer network or stored in his/her directory. Sharing of personal information, such as name, address and phone number can compromise personal safety. The person in whose name a network account is issued is responsible at all times for its proper use. Students and staff may not use anyone else's password, nor may they share their password with others. The school computer network's system operator, or other designated School Board employee, may at any time, review the subject, content and appropriateness of electronic communications or other computer files, and remove them if warranted, reporting any violation of rules to the school administration or law enforcement officials.
- (g) Use of the network shall not disrupt other users on the network.
- (h) Neither hardware nor software shall be destroyed, modified or abused in any way.
- (i) Malicious use of a network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited. There should not be any electronic activity by students that will compromise school facilities, be an interruption of the educational process, or cause undue work by school board employees.
- (j) Hate mail, harassments, discriminatory remarks, profanity, obscenity or language, which is offensive to another user or other antisocial behaviors, are prohibited on the network. Personal Social Media sites should not be accessed during the instructional day. There should not be any content posted on the Internet that causes a disruption of the educational process or involves school district administration.
- (k) The network is protected by Internet filter equipment that restricts users access to materials that are consistent with the standards of

CHAPTER 8.00 - AUXILIARY SERVICES

selection of materials specified in Florida Statutes and with the educational mission, goals, and policies of the school district. These devices block visual displays that are obscene, pornographic or harmful to minors, but this technology is not 100% effective. Use of a network to access or process pornographic materials, inappropriate text files or files dangerous to the integrity of the local area network and/or the wide area network is prohibited. All student network access should be supervised at all times.

- (l) The illegal installation of copyrighted software for use on any district computer is prohibited. Copyrighted material is anything written by someone else. It could be software, an e-mail message, a game, music, a story, or an encyclopedia entry, etc. Students and staff shall not copy and forward, copy and download, or copy and upload to the network or Internet server any copyrighted material, without approval by a school or district administrator.
- (m) The user shall maintain the integrity of the school's/district's electronic mail system. The user is responsible to report all violations. The user is also responsible for making sure all e-mail sent by him/her does not contain pornographic material, inappropriate information, or text-encoded files that are potentially dangerous to the integrity of the local area network or the Internet. Materials received which contains pornographic material; inappropriate information or text-encoded files that are dangerous to the integrity of the local area network or the Internet should be reported to a teacher or an administrator immediately.
- (n) Students and staff shall not infiltrate, or "hack", outside computing systems or networks. Examples: the release of viruses, worms or other programs that damage or otherwise harm an outside computing system or the internal network. Students and staff shall not disrupt a system or interfere with another's ability to use that system (e.g., by sending "e-mail bombs" that cause a disk to fill up, a network to bog down or a software application to crash) nor shall students or staff do any of these things to the Columbia County School District computer system. Financial and legal consequences of such actions are the responsibility of the user (staff or student) and student's parent or guardian.
- (o) Student access to the network or the Internet will be monitored by a staff member.

CHAPTER 8.00 - AUXILIARY SERVICES

- (p) Students shall not access the network or Internet for e-mail, chat rooms, bulletin boards or blogs except while closely supervised by a staff member as part of an educational activity. Students and staff shall not access any type of instant messaging system via the district's equipment or network which would include social media websites such as Facebook, MySpace, LinkedIn, etc. All electronic communications between staff and students must be consistent with the educational purposes of the Columbia County School District.
- (q) Any violation of the use of the Internet shall be reported to the assigned teacher or the assigned principal or administrator.

(3) User Responsibility and Security.

The violations on the preceding pages are only representative. Other forms of misconduct arising from, or connected with, the use of the internet, local area or wide area networks may result in suspension and/or revocation of the offender's privilege of network access.

(4) Disciplinary Action for Violation of Policy

Failure to adhere to these guidelines will result in disciplinary action. Disciplinary action for students will be either Class I, II or III offenses from the Code of Student Conduct. The severity of the violation will dictate the action of the principal. Disciplinary action for school district employees will be handled by the appropriate supervisor.

STATUTORY AUTHORITY:

1001.41; 1001.42, F.S.

LAWS IMPLEMENTED:

1001.43, F.S.

HISTORY:

**ADOPTED: 7/30/02
REVISION DATE(S): 9/13/11
FORMERLY: 2.43**