

## PERSONNEL

File: GAB/IIBE A

### ACCEPTABLE USE OF TECHNOLOGY POLICY

Charlottesville City Schools (CCS) recognizes that technology enhances learning opportunities. CCS provides technology resources for educational purposes only. Use of CCS technology resources, including the CCS network and access to the Internet, is a privilege, not a right. Inappropriate use may result in immediate termination or suspension of access and other privileges relating to the use of CCS technology resources. Inappropriate use may also result in disciplinary action (up to and including suspension or expulsion for students, or formal reprimand, suspension or dismissal for staff) as well as potential civil or criminal liability and prosecution. CCS reserves the right to monitor the use of CCS technology resources, including e-mail communications and access to the Internet, in order to provide an acceptable level of service to all authorized users and to enforce the terms of this policy. Users of CCS technology resources should be aware that data that resides on CCS technology resources or passes through the CCS network is not private and is subject to review without prior notice. CCS is not responsible for any information that may be lost, damaged, or unavailable due to technical or other difficulties. CCS cannot ensure that electronic transmissions are secure and private and cannot guarantee the accuracy or quality of any information obtained using CCS technology resources.

The Charlottesville City School (CCS) division may capture student images, likeness and/or voice on digital media. CSS reserves the right to use this media for promotional purposes unless a student's parent or guardian has withheld consent by completing the Opt-Out Form for Promotional Activities, however student names must not be used in association with this media.

The school division will:

- Provide access to technology resources for students, staff, and other authorized users (as approved by the Network Administrator or designee) who have agreed to abide by the terms of this policy.
- Provide instruction on proper use of technology resources and Internet safety for all authorized users.
- Implement and monitor Internet Safety instruction and curriculum to meet all federal and state mandates. All students and staff will receive instruction in Internet safety including the following topics: personal safety, cyber bullying, cyber security, intellectual property, and copyright. Policy and implementing procedures will be reviewed every 2 years and revision will be made as needed.
- Supervise and monitor student use of the Internet and make an effort to ensure that students access sites with only age- and topic-appropriate materials specifically:
  - Elementary (K-4) staff will make an effort to bookmark sites or use portals to direct students to pre-selected Internet sites.
  - Upper Elementary (5-6) staff will model skills needed to: search for information within an area of study, filter information for credibility and worth, and recognize inappropriate information sources or sites. Teachers will explore Internet sites before directing students to those sites.
  - Middle School (7-8) staff will supervise student-initiated information search activities and provide support as students begin to assume responsibility for

## PERSONNEL

File: GAB/IIBEA

Page 2

becoming independent users of the Internet.

High School (9-12) staff will advise students as they participate in independent Internet use.

- Employ technology protection measures to comply with federal and state mandates to filter or block materials deemed to be harmful to juveniles. However, no known process can control or censor all harmful or inappropriate material that may be available to users of CCS technology resources.
- Provide access to technology resources that allow users to create and post web pages on the CCS network and the Internet. All such web content must follow CCS Web Policy guidelines.
- Provide access to electronic mail for all staff members. Students will not be issued individual e-mail accounts; students should only access e-mail through a teacher-supervised class account. Students may not access personal e-mail or real-time messaging accounts using CCS technology resources unless the student is doing so for an educational purpose and has received explicit permission from a CCS staff member.

Authorized users will:

- Use CCS technology resources in compliance with all local, state, and federal laws including, but not limited to, laws that govern copyright and intellectual property.
- Use CCS technology resources responsibly and with respect for others. Users must leave computers, keyboards, mice, monitors, printers and other peripherals unaltered and in good working condition. Users may not use CCS technology resources to offend, harass, or intimidate others and shall use appropriate language in all communications. Provisions in the student code of conduct will apply to all student interactions with and use of CCS technology resources.
- Use CCS technology resources for educational or job-related purposes only. Users may not use these resources for financial gain, commercial purposes, or political activities unless it is directly related to their job function. Users may not create, distribute, or forward chain letters or hoaxes; nor may users create, distribute, or forward unsolicited bulk electronic communications that are unrelated to the division's educational mission.
- Use only assigned accounts and passwords (where applicable). Users must take appropriate precautions to safeguard account or password information and prevent the use of assigned accounts and passwords by others.
- Maintain the confidentiality and security of protected information. Users may not provide access to confidential information to others who are not authorized to have such information. Users shall be expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential. Employees shall not use e-mail for confidential matters or privileged communications, such as student records, unless appropriate security precautions are taken. A confidentiality statement must be attached to all personally identifiable emails.
- Use student images, likenesses, or voice recordings in digital format in accordance with guidelines.

File: GAB/IIBEA

Page 3

## PERSONNEL

- Maintain the security and functionality of all CCS technology resources. Users shall not attempt to bypass security measures or gain access to unauthorized resources, including, but not limited to, the use of proxy internet sites. Users may not knowingly create or spread malicious code.
- Access, modify, or delete other user's data only after receiving appropriate permission.
- Use CCS technology resources in a way that does not disrupt resource usage by others or monopolize resources. This includes refraining from the consumption of excessive amounts of: network bandwidth, data storage space, and printer supplies.
- Use only software that has been legally obtained, licensed and authorized for use on CCS computers. Users may not download from the Internet, tamper with, copy, install or use any software that compromises the security or functionality of the CCS network or connected networks.
- Access the CCS network utilizing a personally owned computer or other device only after receiving permission from the Network Administrator or designee.

All violations of this policy or problems with any CCS technology resource shall be reported to a teacher, administrator, or other appropriate source. CCS reserves the right to amend this policy at any time and to enforce such amended policy after giving notice of such amendments.

The School Board will review, amend if necessary, and approve this policy every two years.

Adopted: October 21, 1999  
Revised: July 19, 2007  
Reviewed: March 20, 2008  
Revised: June 17, 2010

---

---

Legal References: Code of Virginia, 1950, as amended sections 22.1-78 and 22.1-70.2