

## PERSONNEL

File: GAB/IIBEA-R

### ACCEPTABLE USE OF TECHNOLOGY POLICY

All employees of Charlottesville City Schools shall be expected to receive, review, sign and adhere to the Acceptable Use of Technology Policy.

1. At the beginning of the academic year, access information for the most recently School Board approved policy will be provided by the Coordinator of Media Services to principals for distribution to each new and returning employee.
2. No employee will receive access to any of the school division technology, including user names or passwords, until a copy of the policy has been signed and returned to the Office of Technology.
3. Although included in the policy, the following list of required actions must be followed to maintain access and use of any technology owned by Charlottesville City Schools. If the policy is revised and approved by the Board, the list may be revised accordingly. 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.
  - 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,

## PERSONNEL

File: GAB/IIBEA-R  
Page 2

- 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.
4. Any violations of the policy shall be reported to the employee's supervisor and the Director of Human Resources for possible disciplinary actions.

Issued: August 17, 2009  
Revised: October 11, 2010

---

---

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