



Charlottesville City Schools Acceptable Technology Use Agreement

Charlottesville City Schools (CCS) recognizes that technology enhances learning opportunities. CCS provides technology resources for educational purposes. 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 electronic 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. CCS may capture student images, likeness, and/or voice on digital media in accordance with Community Relations guidelines and Opt-Out procedures. Students and staff should understand when communicating electronically that their screen name, posted photographs, and language represents them online and must meet acceptable standards.

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 may store student and staff information on third party servers in order to use cloud based storage and services. 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.

This agreement supports School Board personnel and instruction policies. Please review policy and regulation GAB/IIBEA online by visiting the Charlottesville City Schools web site (www.ccs.k12.va.us) and navigating to the Policy Manual tab.

Students and families should review Policy Manual Section I - Instruction, links IIBEA and IIBEA-R. Employees and contractors should review Policy Manual Section G - Personnel, links GAB and GAB-R.

The school division will:

- Provide access to technology resources for students, staff, and other authorized users 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.



CHARLOTTESVILLE CITY SCHOOLS

- Implement and monitor Internet Safety instruction and curriculum within the division's instructional program 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, copyright, and networking etiquette. Policy and implementing procedures will be reviewed every 2 years and revisions 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 preselected Internet sites and online activity will be monitored.
 - **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 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.
- Provide access to technology resources that allow authorized users to create and post web pages on the CCS network and the Internet. All such web content must follow CCS Web Policy and Regulations EGAAAA-R. All employees and students shall follow the requirements and responsibilities for the development and use websites and materials described in Policy EGAAAA: Management of School Division Website.
- Provide access to electronic mail for all staff members. Students may be issued individual electronic mail accounts as part of specific instructional programs and initiatives; students should only access electronic mail through a teacher supervised class account.
- Monitor remotely CCS-issued student computer devices within the CCS network to determine appropriate use during the instructional day.
- Monitor the use of CCS technology resources, including electronic 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.
- Leverage technology and/or services to aid in locating and recovering technology that has been reported lost or stolen.

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.



CHARLOTTESVILLE CITY SCHOOLS

- Ensure when downloading, uploading, or importing music, images or videos on district-owned technology during or outside of school hours, that it does not violate copyright law or contain words or images that are pornographic, obscene, graphically, violent or vulgar.
- Adhere to guidelines each time the Internet is used at school and at home on CCS provided hardware.
- 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.
- Be held financially responsible for lost, stolen and/or damaged technology. Assignment of fees will be based on the approved fee schedule.
- Users issued CCS hardware are required to bring a fully charged computer device to school daily as well as electronic media and files required for class.
- Use CCS technology resources responsibly and with respect for others.
- Use only assigned accounts and passwords (where applicable) and take appropriate precautions to safeguard account or password information and prevent the use of assigned accounts and passwords by others.
- Report any security problem or breach to a teacher or administrator immediately.
- Maintain the confidentiality and security of protected information.
- Use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.
- Use student images, likenesses, or voice recordings in digital format in accordance with guidelines.
- Maintain the security and functionality of all CCS technology resources.
- Access, modify, or delete another user's data only after receiving appropriate permission.
- Use only software that has been legally obtained, licensed, and authorized for use on CCS computers.
- Return upon withdrawal from a CCS school or employee termination all issued property prior to leaving the district or as part of the computer collection programs including but not limited to all peripherals, charger & power cords, stylus, carrying case, mice, and keyboard.

Prohibited Acts:

- Computers are to be used for instructional purposes only.
- Students are prohibited from playing games during the instructional day unless otherwise directed to by a teacher or administrator.
- Students are not allowed to connect a portable computer to ethernet jacks in the school unless instructed by teacher or administrator.
- Students shall not save, transfer, or load non-school related materials and files on a school file server or storage system provided by CCS. Students are expected to maintain their instructional files and media in a responsible manner, which includes backing up data and files at regular intervals. USB and other external storage media (e.g.



micro-SD, etc.) can only be used for file storage and shall not be used to launch software.

- User may not use technology resources for financial gain, commercial purposes, or political activities outside of this district purpose. 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.
- Users are not to misrepresent or assume the identity of other users.
- Students and staff will never reveal identifying information, files, or communication to unknown entities through email or posts to the internet.
- Users may not provide access to confidential information to others who are not authorized to have such information.
- Employees shall not use electronic mail for confidential matters or privileged communications, such as student records, unless appropriate security precautions are taken.
- Users will not attempt to bypass security measures or gain access to unauthorized resources or attempt to conceal the identity of one's computer or user information on the CCS network.
- Users will not create or use unauthorized networks including but not limited to voice, data, IP, peer-to-peer, ad hoc, or proxy networks.
- Users will not knowingly create or spread malicious code.

Use of cloud hosted services

Charlottesville City Schools utilize cloud based products to achieve educational goals. Using these tools, students and staff collaboratively create, edit and share files and websites for school related projects and communicate with other students and staff members. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

The use of web-based products in Charlottesville City Schools is governed by federal laws including:

Children's Online Privacy Protection Act (COPPA)

COPPA applies to commercial companies and limits their ability to collect personal information from children under 13. By default, Charlottesville City School's use of cloud based services uses services where advertising is turned off and no personal student information is collected for commercial purposes. This agreement acknowledges that the school will act as an agent for parents in the collection of information within the school context as it applies to cloud based products used in the educational context. The school's use of student information is solely for education purposes.

(COPPA – <http://www.ftc.gov/privacy/coppafaqs.shtml>)



CHARLOTTESVILLE CITY SCHOOLS

Family Educational Rights and Privacy Act (FERPA)

FERPA protects the privacy of student education records and gives parents the rights to review student records. Under FERPA, schools may disclose directory information but parents may request the school not disclose this information.

(FERPA – <http://www.ed.gov/policy/gen/guid/fpco/ferpa>)

Under FERPA and corresponding Virginia law, a student's education records are protected from disclosure to third parties. This agreement is intended as notification that education records stored in cloud services partner domains may be accessible to someone other than the student, staff member, or CCS staff by virtue of this online environment.

This agreement indicates consent to allow student and/or staff education records to be stored by CCS third party vendors providing cloud based services and solutions.

Any violations of this agreement 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 agreement at any time and to enforce such amendments after giving notice of such amendments.

Violations of these items may result in disciplinary action and may also result in criminal charges if the violation is also a violation of Federal, State, or local law or ordinance. Examples of such dual violations are computer hacking or trespassing, harassment, threat, or cyber bullying via a CCS computer, and computer fraud (See title 18.2 of the Code of Virginia). Ignorance of these regulations will not excuse the infraction. Where Virginia law is violated, legal actions may be taken.

Return of Equipment

Failure to return the CCS-issued computer and peripherals in accordance with the stated condition may result in prosecution for all applicable crimes to include, but not limited to grand larceny. Users will be held financially responsible for lost, stolen and/or damaged technology. Assignment of fees will be based on the approved fee schedule.

Adopted: August 1, 2011

Revised: August 1, 2013



Signature Form for CCS Staff

Please keep a copy of the Charlottesville City Schools Acceptable Technology Use Agreement for your reference and return a signed declaration of understanding and adherence to your principal or immediate supervisor.

DECLARATION OF UNDERSTANDING AND ADHERENCE

I understand that I must adhere to the terms of the Charlottesville City Schools Acceptable Technology Use Agreement. I understand that access to CCS technology resources is designed for educational purposes. I accept responsibility to follow policies, regulations and standards for appropriate and acceptable use when I am using CCS technology resources. This agreement for staff, contractors and service providers will be signed at hiring and will remain in effect for the duration of your employment and/or service to CCS or when revisions to the agreement are made.

Date

Name (Please Print)

Signature

School, Department, or Program