

# Technology Acceptable Use Policy

## Clayton County Public Schools

The purpose of this document is to establish a policy to ensure efficient use of CCPS's computer and Internet resources. CCPS provides technical tools and powerful resources to enhance the overall educational experience of its students and educators. There are important rules and guidelines that you must follow to ensure a safe environment. CCPS monitors Internet traffic to ensure optimal use of instructional resources. Following are the rules and guidelines you must follow that govern acceptable behavior when using CCPS's computer and Internet resources. Failure to follow any of these guidelines may result in confiscation of CCPS's resources, suspension of internet access and may also lead to additional action being taken by the Department of Human Resources.

### 1. Computer and Network Resources

**1.1.Ownership.** The computer (laptops, notebooks, desktops, printers, smart devices etc.) and peripherals issued to a Clayton County Public School (CCPS) employee are the property of CCPS and are for employee use only. The computer and peripherals issued to a CCPS employee are to be returned immediately if he\she is no longer employed by CCPS.

**1.2.Use.** The computer and network resources are intended for CCPS related purposes and performance of job duties. The technology acceptable-use policy applies to both work and home use of resources.

**1.3.Personal Use.** Incidental personal use is permitted as long as such use does not violate CCPS's policies as stipulated in this document and does not interfere with school-related performance of job duties.

**1.4.Security.** The user (you) is responsible for all technology equipment issued by CCPS. Technology equipment should be locked and safely stored away when not in use.

**1.5.Computer Loss or Damage.** Promptly report stolen equipment to the Technology Department. In the event of negligent loss or damage, CCPS reserves the right not to issue a replacement computer or peripheral.

**1.6.Accounts and Passwords.** The user should consider the account and password confidential and shall not share the password with any other person. Accounts and passwords may be terminated if appropriate guidelines are not followed.

**1.7. Network File Storage.** Network storage for the “CLAYTON” DOMAIN IS 250 MB per user. This storage is commonly referred to as your “user folder” or “U:/drive”. This folder is **for work related data** only and not for **PERSONAL** files. Applications or programs should not be installed or stored in this location. Files that do not meet the acceptable criteria will be deleted without notification by the Department of Technology.

**1.8. Configuration and Software.** No modifications or configuration changes are to be made to the computer except upon instruction by the Department of Technology. No software is to be installed on the computer except upon approval by the Department of Technology. **Expressly prohibited are peer-to-peer networks such as Kazaa, LimeWire, BitTorrent, and Morpheus or any software installed with the sole purpose of bypassing CCPS’s security policies.**

**1.9 Smart Devices.** Smart devices (Blackberry, ITouch, Palm, etc.,) issued by the Department of Technology are to be used as specified by the signed user agreement form prior to receiving the device. The Technology Department will not support these devices for any other purpose. Non CCPS issued smart devices will not be allowed access to CCPS’s network and will not be supported by the Department of Technology.

**1.10 Employee Data on Local Machine.** CCPS is not responsible for lost or corrupted data in the event of a hardware/software failure or user error. Only data on the “U drive” is backed up. It is the responsibility of the user to maintain a backup of his/her critical data on CCPS equipment. See also: Section 1.7 and 1.8.

**1.11 Student Access.** Students are only allowed on classroom desktops. Educators should use CCPS issued laptops to conduct business. Laptops should be locked when not in use and should not be given to students to perform class work. Students should never be given access to gradebook or any other student data records.

**1.12 Rogue Equipment.** Unauthorized devices such as wireless access points, 3G hotspots, hubs, or routers are considered rogue devices and may not be used. Such devices may interfere with the CCPS network WAN/LAN. Additionally, do not plug in any network cables without consent from the Department of Technology.

## 2. Electronic Mail Resources

**2.1. Purpose.** Electronic mail (email) is provided to the staff of CCPS (users) to facilitate information exchange consistent with the educational mission of CCPS.

**2.2. Property.** The email system, computers, and user accounts and addresses are the property of CCPS.

**2.3. Privacy.** Users do not have a personal privacy right in any matter from the email system. CCPS may at times and without prior notice, monitor and review email by users.

**2.4. Confidentiality.** The confidentiality of email cannot be assured. Such confidentiality may be compromised by applicability of law or policy, by forwarding of email, or because of unauthorized access. Users, therefore, should exercise caution in using email to communicate confidential or sensitive matters.

**2.5. Outlook Web Access.** CCPS provides access to its email via a web browser. If you are using a device other than the device provided by CCPS, it is imperative that appropriate security software (enterprise anti-virus and anti spyware) is loaded on the device. Please consult the Department of Technology for additional information if needed.

**2.6. Storage.** The outlook storage size for the "CLAYTON" domain is 250MB or 500MB (for administrative employees). Users are encouraged to store large attachments received via email into another location (U-drive/hard drive/external drive). After attachments have been saved, original emails can be deleted to free up space in the mailbox.

## **2.7. Restrictions.**

**2.7.1.** Users may not use email in any way inconsistent with or in violation of the policies set by CCPS.

**2.7.2.** Users may not use email for unlawful activities, commercial purposes or personal financial gain.

**2.7.3.** Users may not deliberately disrupt email services or perform activities that interfere with the use of emails by others.

**2.7.4.** Users of the email system shall not use email in any way that would be considered (a) damaging to another person's reputation, (b) abusive, (c) obscene, (d) sexually orientated, (e) offensive, (f) threatening, or (g) Harassing. *(CCPS has many tools in place to monitor and control the flow of e-mails, but cannot guarantee that a user will not receive an offensive email)*

**2.7.5.** Users may not seek, use, or disclose personal or confidential student or employee information except for proper school system business.

**2.7.6.** Users may not send mail to more than 150 addresses at a time. Mail should be sent to a targeted user or group. CCPS email resources may not be used for personal gain or enterprise. Examples include political campaigning and business solicitations.

**2.7.7.** Users may not create, forward or reply to "chain letters" or similar email. "Chain letters" include but are not limited to "Get Rich Quick", "Feel Good", "New Virus Hoax", and "Good Luck" letters. If you receive such emails, simply delete it from your inbox.

**2.8. Personal Use.** CCPS email services and accounts may be used for incidental personal purposes provided that such use complies with CCPS policies. CCPS does not guarantee access to

private email accounts. Additionally, such use shall not burden the operation of the email system or add to the cost of such operation. Emails arising from such use is the property of CCPS.

## **2.9 Spam Email – Unsolicited emails**

**2.9.1 “Phishing”** is a method of spam email that attempts to persuade the user into disclosing sensitive information such as network username and password. Please be advised that this type of email does not originate from the Technology Department. **The Department of Technology will NEVER ask for your username and password via email. Disclosing or compromising your network username and password is significant and can negatively affect our entire email system.**

## **3. Internet Resources**

**3.1.**Users will use appropriate language on the Internet.

**3.2.**Users will not access or transfer inappropriate materials. Internet traffic is monitored and abuses will be reported.

**3.3.**Users will respect and uphold copyright laws.

**3.4.**Downloading games, video files, audio files or running streaming media without educational value and without approval from the Department of Technology is prohibited. Streaming media is bandwidth intensive and can negatively affect important internet based applications if not used properly.

**3.5** URL filtering is maintained in compliance with the Children’s Internet Protection Act regulations. No attempt should be made to circumvent security measures in place. Contact the Department of Technology should you need access to a site currently blocked by the URL filter.

## **4. Web Development**

**4.1.**School and/or Teacher websites may NOT publish photos on pages without consent from all individuals and their parents/guardians.

**4.2.**Teachers may not link to their own personal pages to pages associated with CCPS.

**4.3.**No student email addresses, home addresses or phone numbers shall be on any web pages.

**4.4.**No marketing or advertising may be done on Teacher or School websites except for Partners in Education

4.5. Teachers, webmasters and Principals assume all responsibility for all content displayed within the schools' and the teachers' websites.

**5. External Storage (USB devices\External HD)**

5.1 Educator\Department of Technology must periodically audit external storage devices

5.2 Only files pertaining to class room activities may be stored on external devices

5.3 Virus scans must be performed prior to the use such external devices

5.4 CCPS's IT department is not responsible for recovering data that resides on external devices

5.5 Confidential or sensitive data (student data, Social Security numbers, employee data) belonging to CCPS must not be copied to external storage devices.

I understand and will abide by the terms and conditions as stipulated by this document for using technology in Clayton County Public Schools. I understand that any violation of the regulations may result in disciplinary action against me and may also constitute a criminal offense. I understand that I must adhere to Board Policies BH/GAG, GAHB, GBU, IFA(1), and any other applicable board policies when using CCPS's Computer and Network Resources, Electronic Mail Resources, Internet Resources or Websites.

For Technology related help please contact: [ITHelp@clayton.k12.ga.us](mailto:ITHelp@clayton.k12.ga.us) or 770-473-2772 Ext. 2

For future reference view online at [www.clayton.k12.ga.us/AUP-somelocation](http://www.clayton.k12.ga.us/AUP-somelocation)

---

Print Name of Employee

Employee's Signature

Date

Last Revision - May, 2010