

STUDENT REQUIRED USE OF TECHNOLOGY & INTERNET SAFETY POLICY**INTRODUCTION**

The use of new technologies presents new possibilities and challenges for the mission of the Cincinnati Christian Schools. With the growth and ever-expanding presence of technology in our world, CCS strongly believes in the incorporation of these resources into our curriculum and instruction. It is vital to equip our students with the knowledge, skills, and expertise necessary to maximize the potential of technological tools in their education. To ensure that technology is being used for its intended purpose at CCS and that conduct reflects this purpose, CCS has created the **Student Required Use of Technology and Internet Safety Policy**. This policy serves as the official guideline for the appropriate use of technology in terms of utilization, behavior, and consequences for misuse.

Reflected in the Core Values of Cincinnati Christian Schools is the notion that while we partner with parents in the education of our students, they, the parents, have the primary and ultimate responsibility for the education of their children and their behavior. A positive, safe, and accepting environment is conducive to maximum learning. Students must learn self-control, respect for authority, and to take personal responsibility for their own actions and behavior.

GENERAL INFORMATION FOR USERS OF TECHNOLOGY

CCS uses new technologies, electronic resources, and Internet access to enhance student learning and to provide a quality educational experience for all students. CCS has been provided with Internet connectivity through service that is partially funded by the Legislature of the State of Ohio and the Federal Communications Commission. Therefore, Internet access and activities utilizing all other technologies in our schools is strictly limited to educational purposes.

Consistent with the mission of Cincinnati Christian Schools to provide a Christ-centered 21st century education, the school will monitor, instruct about, and guard against inappropriate, unethical, and illegal use of technology by student and adult users alike.

REQUIRED USE OF TECHNOLOGY AND INTERNET SAFETY POLICY**GENERAL**

- CCS must have on file a signed *Required Use of Technology and Internet Safety Policy Acknowledgement Form* for any student using technology resources, Internet accounts, school-sponsored accounts, or personal accounts to access the Internet. All Internet access and use of other electronic communication technology is strictly limited to educational purposes. These must be signed and submitted each school year.
- CCS adheres to the *Children's Internet Protection Act*, which is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers.
- CCS has right of access to any electronic devices on school property or owned by the school. All information received or sent from school property remains the property of the school and is not considered confidential. The school reserves the right to investigate the download history of all school computers. There shall be no reasonable expectation of privacy.

EMAIL, WEB BROWSING, AND SOCIAL NETWORKING

- Students (including those over 18) are not allowed to access personal email accounts at school.
- Social networking sites are not to be accessed by students at school.
- CCS realizes that social networking sites and blogs are popular and that they present an opportunity to share with others in a positive way. However, abuses can occur. Therefore, this policy applies to all Internet communications available to the public.
- All Internet communications are subject to this policy and the policies in the *CCS Parent/Student Handbook* with the understanding that students represent CCS at all times, not just during school hours.

SCHOOL RESPONSIBILITY

The school shall provide access to technological resources, including the Internet, for educational purposes only. CCS shall also provide training for students in the appropriate use of technology. CCS does not guarantee the accuracy of information gathered from school computers or the Internet. CCS shall take measures to provide for the safety and security of minors, supervise and monitor student access to all technological resources provided by the school, and guard against the access of objectionable material, in compliance with the *Children's Internet Protection Act*. CCS will provide filtered Internet access and will monitor student Internet access in accordance with the law. Unauthorized disclosure, use, and dissemination of personal information regarding minors is forbidden.

STUDENT RESPONSIBILITY

Specifically, the student:

- Will make available his or her laptop for inspection by an administrator or teacher upon request. Messages or files sent or received at any Internet location as well as files stored and information accessed, downloaded or transferred on CCS-owned technology are not private.
- Will access CCS technological resources for educational purposes only.
- Will not share passwords or attempt to discover passwords. Sharing a password could make students liable if problems arise with its use and subject to disciplinary action.
- Will strictly adhere to copyright laws and only download/import music or other files to a CCS owned technology device that he or she is authorized or legally permitted to reproduce, or for which he or she has the copyright.
- Will only use the Laptop for ethical and legal purposes.
- Will refrain from unauthorized access, including hacking or use of another person's account.
- Will not bypass the school firewall and/or filtering, nor harm or alter school property.
- Agrees not to pirate, nor to submit, publish, and/or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, harassing, racially offensive or otherwise illegal material, on or off school property; nor shall the user encourage the use, sale, or distribution of controlled substances.
- Is responsible for any Internet-based communications that adversely reflect on the students' or school's Christian testimony, that contain confidential school information, that disparage the school or its students or staff, or that violate the school's anti-discrimination, anti-harassment policies. Behavior of this sort may result in requests to remove the communication and in disciplinary actions.

Student Responsibilities continued:

- Is responsible for information that is sent and received under his/her personal and/or school Internet account.
- Is personally responsible for all material that he/she posts on a website or for content posted by third parties to the student's social networking or other Web pages.
- Will not connect any personal technologies such as laptops and workstations, wireless access points and routers, printers, etc. to CCS owned and maintained local, wide, or area networks. Home Internet service is the responsibility of the student both in cost and configuration.
- Will keep the laptop secure and damage free. Each laptop is issued with a protective case that must be used at all times. Laptop must be in a closed-lid position when carried. Failure to use the case will result in disciplinary action.
- Will not tamper with computer hardware or software; engage in unauthorized entry into computers, nor vandalism or destruction of the computer or computer files.

DISCIPLINARY ACTION

CCS may take disciplinary action against any student who violates *the Required Use of Technology and Internet Safety Policy* or other policies by means of inappropriate use of technology. Disciplinary action may also be taken against those who use telecommunication devices to cause mental or physical distress to other members of the school community, whether these incidents take place on or off the school property. Disciplinary action taken by school authorities may include revocation of access to technological resources, suspension, expulsion, and/or possible legal action.

Within reason, freedom of speech and access to information will be honored. During school, teachers will guide students toward appropriate materials. According to school policy and procedures, the following are not permitted:

- Submitting, publishing, and/or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, harassing, racially offensive, or otherwise illegal material, on or off school property.
- Using the CCS network, e-mail, or instant messaging (on any electronic device) for cheating and/or communicating during tests or exams.
- Unauthorized use of translation software or on-line translations.
- Using another person's password or login and/or trespassing in another person's folders, work, or files.
- Impersonating another on any social networking sites, blogs, wikis, or interactive sites of this kind.
- Violating copyright laws.
- Accessing inappropriate matter on the Internet or World Wide Web.
- Unauthorized access, including so-called "hacking" or "pirating" and other unlawful activities online.
- Abusing or wasting limited resources.
- Downloading and/or installing non-approved programs or video files on school computers.
- Using chat rooms, online or instant messaging while at CCS or in the CCS network or on any CCS computer or any other device unless assigned and supervised by a member of the faculty or staff.
- Access to non-school e-mail accounts.
- Employing the network for non-educational and/or commercial purposes.
- Using the CCS network to promote individual benefits or outside fundraising not pertaining to CCS.
- No teacher or student shall be recorded by students without that person's explicit permission.