CHARLOTTE CHRISTIAN SCHOOL
veritas tota homini toti

Responsible Use Policy

7301 Sardis Road – Charlotte, NC 28270 – (704) 366-5657 – (704) 366-5678 Fax – www.charlottechristian.com

PURPOSE

Charlotte Christian School's intention for publishing a Responsible Use Policy is not to impose restrictions that are contrary to the established culture of spiritual maturity, trust and integrity. The purpose of this policy is to outline the acceptable use of Charlotte Christian School information technology resources for the protection of all parties involved.

SCOPE

This policy applies to all faculty, staff, and students at Charlotte Christian School. Volunteers using school equipment to complete school-related activities are also covered by this policy. These guidelines also apply to any and all use of Charlotte Christian School information technology resources, including but not limited to the following: computer systems, mobile devices, e-mail, network resources, and internet connections.

ELECTRONIC COMMUNICATION

Use of Charlotte Christian School's electronic communications is permitted as long as:

1. such usage does not negatively impact the Charlotte Christian School computer network and,

2. such usage does not negatively impact parties involved.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive but is included to provide a frame of reference for the types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary should not be sent via email without encryption.
- It is Charlotte Christian School policy not to open email attachments sent from unknown users or when such attachments are unexpected. If in doubt…don't.
- Email systems are not designed to transfer large files and as such emails should not contain attachments of excessive file size. Use Google Docs, Dropbox, etc. for sending large files.
- Access to social media without teacher approval during class time is prohibited.

- Photos, video and/or sound recording, during class time without teacher/administration permission is prohibited.

STUDENT EMAIL ACCOUNTS

Students in grades 9-12 will be issued email account credentials. The email account is for school-related use and activities only. Personal email accounts should be used for non-educational communication. Please observe the following:

- Be polite. Do not use abusive, offensive or inappropriate language.
- Email etiquette should be observed. Only send messages that one would say verbally to the recipient.
- Students who receive harassing or threatening messages should notify a faculty or staff member immediately.
- Mailing lists are for school use only. Student use of email lists are not permitted without the approval of the school administration.
- The use of email in class without teacher permission is strictly prohibited.
- Bulk emails are prohibited.
- Never include personal information such as home address or phone number.
- Attempts to read, delete, copy or alter email of other users are prohibited.
- School email addresses are not to be given to any website, company or third party without the permission of school administration.

CONFIDENTIALITY

Confidential data including username and passwords must not be shared or disclosed in any manner, posted on the internet or any publicly accessible systems, or transferred in any insecure manner. It is dangerous to disseminate personal information such as full name, date of birth, address, etc. in an online setting.

NETWORK ACCESS

Network access is a privilege and not a right. Users should only access network resources that are applicable to them. Existence of access capabilities does not imply permission to use this access. Charlotte Christian School is not responsible for data loss on network devices.

UNACCEPTABLE USE

The following shall constitute unacceptable use of Charlotte Christian Information Technology resources. The user may not:

• Engage in any activity that is illegal under applicable laws.

• Engage in any activity that may cause embarrassment, loss of reputation or other harm to Charlotte Christian School.

• Disseminate defamatory, discriminatory, sexist, racist, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate messages or media. All such instances should be reported to a faculty or staff member immediately.

• Engage in activities that cause disruption of the learning environment.

• Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging or other IT information gathering techniques when not part of the employee’s job function.

• Install or distribute unapproved, unlicensed or “pirated” software.

• Engage in activities that could harm the network or IT devices.

• Play executable computer games.

• Students are not to use another person’s credentials to gain access to the Charlotte Christian School network, internet, another user’s files, or to impersonate another user.

WEB BROWSING

The internet is a collection of interconnected computers that is dynamic. The user should recognize that all information is public domain and the user can inadvertently come into contact with information that some users could find offensive. While Charlotte Christian School filters internet information using constantly updating software, it is impossible to block/filter all offensive sites. Users then must understand that they are using this resource at their own risk. Users should take reasonable safeguards when using the internet and also recognize that not all information is accurate and Charlotte Christian School is not responsible for the quality or validity of information accessed. If a user inadvertently accesses obscene or objectionable material, the user should immediately notify a faculty/staff member and the director of technology and innovation so that the material can be blocked from further access.

COPYRIGHTED MATERIAL

The Charlotte Christian School IT resources must not be used to download, upload or otherwise handle illegal and/or unauthorized copyrighted content.

PEER-TO-PEER FILE SHARING

Peer-to-peer networking (Including, but not limited to Airdrop) is prohibited on Charlotte Christian School's network and devices unless authorized by a teacher for a specific file transfer.

DISTANCE LEARNING / VIRTUAL CLASSROOMS

Distance learning is considered an extension of our main campus and is used as a tool to enhance learning. When meeting with teachers and other peers in a virtual environment, students are expected to adhere to all CCS policies. Normal classroom and responsible use policies apply both on campus and in virtual meetings and classrooms. Participation of all users (students and guests) in a virtual meeting is at the sole discretion of the teacher host. Any disruption to a video conference class or meeting is prohibited.

EXPECTATION OF PRIVACY

Users should expect no privacy when using Charlotte Christian School's network. Such use may include, but is not limited to, transmission and storage of files, data, and messages. Charlotte Christian School reserves the right to monitor any and all use of the network. To ensure compliance, this may include the interception and review of any emails, or other messages sent or received as well as inspection of data stored on personal file directories, hard disks and removable media.

DEVICE SECURITY

- Students must receive prior permission before borrowing any device or accessories. Failure to comply will be considered theft and the student will be referred to the administration for disciplinary action.
- Students are responsible for their computing device and accessories including but not limited to chargers and batteries.
- Student computing devices should not be left unattended at any time. Devices that are not being monitored by the student should be secured in an appropriate manner.
- Users are responsible for backing up their own data. Lost or damaged data is not the responsibility of Charlotte Christian School or the Technology and Innovation Department.

CIRCUMVENTION OF SECURITY

Using IT systems to circumvent security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is also expressly prohibited. If an individual becomes aware of such activities, the individual should immediately alert a faculty or staff member who will then notify the Technology and Innovation Department.

SOFTWARE INSTALLATION

In an effort to limit security threats such as malware, spyware, trojans, etc. only Charlotte Christian School approved software may be installed on systems. Installing unapproved personal items/software is considered irresponsible and unacceptable use. ALL software installed must be approved by the Charlotte Christian School Technology and Innovation Department.

ILLEGAL ACTIVITIES

No Charlotte Christian School IT system may be knowingly used for activities considered illegal under local, state, federal, international or other applicable laws. Such actions may include but are not limited to:

- Unauthorized port scanning
- Unauthorized network hacking
- Unauthorized packet sniffing
- Unauthorized packet spoofing
- Unauthorized wireless hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a system
- Acts of terrorism
- Identity theft
- Spying
- Downloading, storing or distributing violent, lewd, perverse, obscene or offensive material
- Downloading, storing or distributing copyrighted material

ENFORCEMENT

Violations may result in disciplinary action including but not limited to suspension, restriction of access, expulsion, or termination as determined by school administration.

DIGITAL EDUCATIONAL ENVIRONMENT AGREEMENT

Charlotte Christian School utilizes the internet and a variety of online tools that enable students and teachers to teach, to learn, and to collaborate in a digital educational environment. In addition to Google Apps for Education, Canvas, and SeeSaw; other educational websites, applications, and virtual conferencing platforms are used to enhance learning. All provisioned accounts will be created and maintained by the school. In compliance with the Responsible Use Policy as well as the federal laws listed below, Charlotte Christian School reserves the right to supervise, filter, and monitor school-issued student accounts and online activity.

CHILD INTERNET PROTECTION ACT (CIPA)

Charlotte Christian School is required by CIPA to have technology measures and policies in place that protect students from harmful materials. Therefore, Charlotte Christian School will filter content from inappropriate websites and will monitor student data and productivity and will operate in full compliance of CIPA.

CHILDREN'S ONLINE PRIVACY PROTECTION (COPPA)

COPPA limits the abilities of commercial companies from collecting personal information from children under the age of 13. Therefore, Charlotte Christian School will create all student accounts, disable advertising for all users, and will not allow any personal student information to be collected for commercial use.

Updated as of March 27, 2020