Acceptable Use Policy

Introduction

Capital Christian Center (CCC) and School (CCS)—also referenced as the Enterprise—recognize that access to technology gives students and staff greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students and staff develop 21st Century technology and communication skills in a God-honoring manner. To that end, we provide access to technologies for student and staff use.

This Acceptable Use Policy outlines the guidelines and behaviors that students and staff are expected to follow when using technology tools (desktop, laptop, phone, tablet, etc.) in school or on CCC/CCS's campus.

- CCC/CCS wireless network is intended for educational and staff purposes.
- Activity over the network or using school technologies will be monitored and may be retained.
- Access to online content via the network is restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students and staff are expected to follow the same rules for good behavior and respectful conduct online as offline.
- CCC/CCS make a reasonable effort to ensure student and staff safety and security online but will not be held accountable for any harm or damages that result from use of school and campus technologies.
- Students and staff are expected to alert school faculty or administration immediately of any concerns for safety or security.
- Failure to comply with the AUP may result in disciplinary action.

Using Desktop, Laptop, Phone and/or Tablet

All technologies provided by or used at CCC/CCS are intended for educational and ministerial purposes. Students and staff are expected to follow the biblical mandate to honor the Lord Jesus Christ in all they do. Therefore, we expect students and staff to use technology in a way that is safe, appropriate, careful and kind. Students and staff should not try to get around technological protection measures, should use good common sense, and should ask if questions arise. Inappropriate uses of technologies and social media is subject to discipline.

Hot Spots and 3G/4G/5G

Students are not permitted to connect to the Internet using a detected hotspot or 3G/4G/5G account while at school. Users must use available Wi-Fi while on school grounds.

Responsibility with Devices

1. If students leave their device at home, they are responsible for getting the course work completed as if they had their device present.
2. Loaner devices may be available to students in grades 6-12 who forgot to bring theirs to school or failed to charge them.
3. On school-owned loaner devices, students may not download apps (including, but not limited to, games, music, or social media) unless directed by or with the permission of a teacher.
4. Students who repeatedly fail to bring the device to school or fail to maintain a fully charged battery will be subject to discipline as determined by administration.
5. Each student is responsible for his/her own device: set up, maintenance, and charging. Teachers are not responsible for storing student devices at any time, nor will any CCS employee diagnose, repair, or work on a student's personal device.

Passcodes and Passwords

1. Students must not share their passwords/passcodes/login information with any other student at any time for any reason.
2. Students may not attempt to use another student's or staff member's account at any time for any reason.
3. Assigned passwords may not be altered unless otherwise instructed by an authority figure.

Sound/Music

1. On all student devices, sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
2. Students are not permitted to use earbuds or headphones of any kind on campus during school hours unless the classroom teacher has granted permission for instructional purposes in the classroom setting.

Recording

1. The use of audio, video, and/or pictures of teachers, staff, administrators, or students is **NOT** permitted without consent. For example, you may not record or video a class lecture without receiving prior permission from the instructor. Violations will be subject to discipline. (California Code, Education Code - 51512)
2. Under no circumstances should recording take place in bathrooms or locker rooms. Violations will be subject to discipline.

Device Use and Inspection

1. Students are **NOT** permitted to use gaming or social media apps during class time in high school or during school hours at the K-8 level.
2. Use of devices should not disrupt the concentration of other students or staff at any time.
3. Students are **NOT** permitted to airdrop on campus at any time.
4. Students are **NOT** allowed to download or stream music or games during school hours or to participate in anything non-academic unless instructed by faculty for educational use.
5. Teachers and staff always reserve the right to ask students to check devices anytime while on campus.
6. Students may be selected to provide their device for inspection for safety and security purposes at the discretion of the Enterprise. **Do not assume any privacy right in any information that is uploaded or downloaded temporarily or permanently stored in the system.**
7. Cell phones are not an acceptable device for use in the classroom during school hours. For K-8 students, cell phones are not to be used on campus during school hours. Smartwatches are considered a cell phone equivalent and should be treated as such.
8. Translators may only be used for translating purposes and must not have Wi-Fi or Internet capabilities. These pre-approved devices must be data-based only.

Printing/Wireless Printing

1. Printing may be available with teacher permission only. Students (6-12) given permission to print will only be allowed to print in the K8/HS libraries at designated student printers for a nominal fee.
2. Printing classwork is the students' responsibility; school printing may not be guaranteed.

Cloud Drives

1. Students are responsible for ensuring that work is not lost due to mechanical failure, failure to back-up files, or accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work; therefore, students should back up all work to the Cloud.
2. The teachers may grant students access to share their work through the Cloud. The students should not attempt to bypass any restrictions to gain access.

Network Access/Connectivity

1. Students and staff are required to connect to the wireless network using the provided user name and password given from the Capital Christian Enterprise IT Department. CCC/CCS makes no guarantee that the wireless network will be operational 100% of the time.
2. Students in grades 6-12 and staff may bring and use personal, portable, electronic devices. Devices such as, but not limited to, electronic readers, small laptop computers, cell phones, or any other portable equipment can access the CCS filtered Wi-Fi network. (Refer to campus-specific handbooks for additional policies.)

Web Access/Filters

1. CCC/CCS provides students and staff with access to the Internet, including websites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored, and web activity records may be retained indefinitely.
2. Students and staff are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a student or staff member believes it shouldn't be, the student or staff member should alert a member of school faculty or administration. If an attempt is made to circumvent the filtering software with any, but not limited to, proxy and/or VPN service, network access privileges may be revoked.
3. If students or staff members come across anything they think the school would deem inappropriate, they should notify an administrator immediately.
4. Parents are encouraged to use safety features to limit or disable specific use of their student's device.

E-mail

1. CCC/CCS will provide students and staff with an e-mail account (name@k12cougars.cc, name@capitalchristian.school , or name@capitalonline.cc) for the purpose of school-related and Enterprise communication. Availability and use may be restricted.
2. Student and staff e-mail accounts should be used with care. Students and staff should not send personal information, should not attempt to open files or follow links from unknown origin, should use appropriate language, and should only communicate with other people as allowed by the Enterprise or their teacher.
3. Students and staff are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. E-mail usage may be monitored and archived.

Security

1. Students and staff are expected to take reasonable safeguards against the transmission of security threats over the campus network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.
2. If students or staff members believe a device might be infected with a virus, they need to alert the Help Desk. They should not attempt to remove the virus themselves or download any programs to help remove the virus.

Netiquette

1. Students and staff should always use the Internet, network resources, and online sites in a courteous and respectful manner.
2. Students and staff should also recognize that along with valuable content online there is also unverified, incorrect, or inappropriate content. Students and staff should use trusted sources when conducting research via the Internet.
3. Students and staff should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's accessible and can be shared and spread in ways the original user never intended.

Plagiarism

1. Students and staff should follow all copyright laws in the use, installation, distribution, duplication, or modification of copyrighted material. Failure to do so is considered plagiarism.
2. Plagiarism is taken very seriously; strict consequences apply if a student plagiarizes. These consequences are outlined in the Student Handbook.
3. A plagiarism content filter called "Turnitin" is used as a resource for our students.

Personal Safety

1. Students should never share personal information (including, but not limited to, phone number, address, social security number, birthday, or financial information) over the Internet without adult permission. Students should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others.
2. If students see a message, comment, image, or anything else online that makes them concerned for their personal safety or the personal safety of another, they should bring it to the attention of an adult (teacher or staff if they're at school; parent/guardian if they're using the device at home) immediately.

Cyber-bullying

1. Cyber-bullying will not be tolerated. Harassing, dissing, denigrating, impersonating, pranking, excluding, and cyber-stalking are all examples of cyber-bullying. Additionally, sending emails or posting comments with the intent of scaring, hurting, or intimidating someone else are also considered cyber-bullying and will not be tolerated.
2. Engaging in cyber-bullying behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges, potentially up to expulsion from the school. In some cases, cyber-bullying can be a crime. Remember that all activities are monitored and retained. (California Code, Education Code - 48900)

Social Media

1. Whether on or off campus, students and staff are prohibited from violating school rules and policies through social media (including harassment and bullying) on school or personal devices.
2. Defamation of others through social media (or any other platform) in the school community is prohibited.
3. Neither students nor staff may disclose private information of students, employees, or families through social media (or any other platform).

Parent/Guardian Responsibilities

In partnership with the school, it is expected that parents talk with their children about values and the standards students should follow on the use of the Internet just as on the use of all media information sources such as television, cell phones, videos, movies, and music.

Examples of Acceptable Use

I will

- Never leave my device unattended, and I will know where it is at all times. I will place some form of name identification on the case or device itself in the event that the device is found.
- Use Enterprise technologies for Enterprise-related activities.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat Enterprise resources carefully, and alert staff if there is any problem with their operation.

- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use Enterprise technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of Enterprise technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of Enterprise resources.

This is not intended to be an exhaustive list. Students and staff should use good judgment when using any technology.

Examples of UN-acceptable Use

- Spamming: sending mass or inappropriate messages of any kind
- Gaining access to other accounts, files, and/or data
- Using the Enterprise's Internet/E-mail accounts for financial or commercial gain or for any illegal activity
- Participation in credit card fraud, electronic forgery or other forms of illegal behavior
- Vandalizing (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of Enterprise equipment
- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients
- Bypassing the Enterprise's web filter through a web proxy, 3G/4G or Hotspot
- Removing the device profiles and restrictions from the device
- Using another student's or staff member's device
- Installation or transmitting copyrighted materials illegally
- Violates any existing Enterprise policy or public law
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials
- Using chat rooms, sites selling term papers, book reports, and other forms of student work
- Gaming during class or work
- Attempting to find inappropriate images or content
- Engaging in cyber-bullying, harassment, sending sexually explicit photos, arranging to meet someone online or disrespectful conduct toward others
- Trying to find ways to circumvent the Enterprise's safety measures and filtering tools
- Agreeing to meet someone met online in real life
- Using Enterprise technologies for illegal activities or to pursue information on such activities
- Attempting to hack or access sites, servers, or content that isn't intended for the user

This is not intended to be an exhaustive list. Students and staff should use their own good judgment when using any technology.

Limitation of Liability

Capital Christian Center and School will not be responsible for damage, harm or theft to student-owned devices. While Capital Christian Center and School employs filtering and other safety and security mechanisms and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Capital Christian Center and School will not be responsible, financially or otherwise, for unauthorized transactions conducted over Capital Christian Center's network.

Violations of this Acceptable Use Policy

Violations of this Acceptable Use Policy may have disciplinary repercussions, including, but not limited to

- Suspension of network, technology, or computer privileges
- Notification of parents
- Detention, suspension, or expulsion from school and school-related activities
- Employment termination
- Legal action and/or prosecution

Glossary

Term	Description
App	Short for 'application'. This is the primary word used to reference programs that run on a tablet or smartphone. This is synonymous with 'program' for conventional computers like laptops or desktops. *Apps* can be free or cost money just to download. *Apps* that are initially free often offer additional functionality via *in-app purchases* or through a *subscription service*. Some paid *apps* may also offer *in-app purchases* or *subscription services*.
Back-Up	1) The process of making a copy of an original file in case the original file is lost 2) the copy of an original file. *Back-ups* are only a back-up if the original file is not deleted. *Back-ups* can be made to a variety of locations: external hard drives, flash drives, SD cards, *cloud storage*, etc.
Blog	Short form of 'web log'. A *blog* is normally a regularly-maintained website with updated information about a particular person or organization. *Content* and format can vary greatly.
Chat	Online dialogue between 2 or more persons. This can be public or privately viewed.
CIPA	Acronym for Children's Internet Protection Act, enacted by Congress in 2000, meant to address concerns to minor's access to explicit *content* on the Internet.

Cloud Storage	An online location (sometimes simply a network folder) used to store information. The longest-running example of a *cloud storage* system is e-mail.
Comment	Usually this is an online response within a *forum* or a *threaded discussion* to an initial *post*. Some *comments* can be in the form of an image or link to other *content*.
Connectivity	The relative strength, speed, and/or consistency of Internet access.
Content	In the context of computer terminology, a general category for any item that is provided by a website or *app*. This is a wide category and can include files, other apps, images, etc.
Cyber-Bullying	An umbrella term used to explain bullying over the Internet and/or *social media*.
Cyber-Stalking	Stalking someone utilizing online resources.
Data Privacy	The privacy of *personal information*.
eBook	This is a digital format for a book. Not all books are available in eBook format. Most eBooks need an *app* to view them.
Forum	Generally, this is an online dialogue among several individuals regarding a particular topic. Often, these are a discussion regarding an initial *post*.
Hotspot	An electronic device that is sometimes built into a smartphone or some tablets that enables the user to broadcast local wireless Internet. Aside from the physical *hotspot* devices themselves, users generally have to pay extra for this service through a *provider*.
ISP	Acronym for Internet service provider.

In-App Purchase	Some *apps* offer additional features that are not free. These can occur with free or paid *apps*. These additional features are *in-app purchases*.
Meme	An Internet style of joking that plays upon images that have a specific theme or joke that corresponds to them. Often, memes are images that have text typed upon the image itself; the text usually has a common format or word order associated with a particular image. The primary function of memes is usually to deliver a joke. Additionally, some memes can simply just be the common text format or word order itself, applied to any image that can be related to it, even if only obscurely.
Net	In the context of computer terminology, this is short for 'Internet'; the worldwide web.
Netiquette	A concatenation of the words "net" and "etiquette"; i.e. online etiquette.
Passcode	1) Synonym for password; generally (but not always) required with a username; 2) a code needed to access a special service, website, or app; sometimes grants special privileges.
Personal Information	Any piece of information (usually electronic information) that is unique to an individual (e.g., e-mails, passwords, credit card numbers, account logins, etc.).
Post	A general category for any written work "posted" online. This can be as short as a single sentence (e.g. a Twitter or Facebook 'post') or lengthy work in a blog or online article.
Profile	A set of information specific to an individual. The degree of information needed for a profile can vary as well as the function of a profile. Sometimes a profile is simply a set of settings for a user with no personal information attached.
Provider	An abbreviation for "Internet Service Provider"; a company that provides Internet services. See ISP.

Security Threats	A category of items that potentially compromise data privacy or harm a device or computer's functionality. Examples include: spyware, viruses, adware, worms, trojans, hackers, peer-to-peer networks, etc.
Social Media	A category of websites and apps used for social networking (e.g. Facebook, Twitter, Snapchat, Instagram, etc.) The format and function of these can and continues to vary greatly.
Subscription Service	A category of items that require periodic payment to operate. Phone, cable, or Internet service are basic examples of subscription services. In the context of apps or programs, many companies may offer free software to install, but also require a paid subscription to use them (e.g. Microsoft Office programs, Adobe Photoshop, etc.).
Web Access	Access to the Internet.