

Technology Requirements and Acceptable Use Policy 2021-22 (Found in the CCA High School Parent/Student Handbook)

High school students are required to bring a laptop for personal use throughout the school day. Requirements are:

- Intel Core i5, 8th Gen or Better
- 8 GB Ram
- 128 GB Hard Drive or SSD Storage
- Windows Based PC – Recommended
- 14" or larger Display

(Macs will work, but teachers may use a software only available on Windows, so Windows is recommended.)

- Chromebooks and iPads are **not** recommended.

Access to the Internet is a wonderful opportunity to interact with the world. The opportunity brings with it many responsibilities. To use the internet services at Concordia Christian Academy, a student must agree by signature to the following: (Form available in the school office.) All students using CCA or personal computers, personal Mobile Learning Devices (MLDs) and the Internet agree to abide by the following policy:

Purpose

1. CCA computers are available for academic use consistent with the mission and purpose of Concordia Christian Academy as a Christ-centered environment. Electronic devices and resources are intended to help students grow in the use, understanding, and appreciation of technology, and to enhance research skills.
2. Personal or school computers and personal MLDs are not to be used for any illegal, commercial, for profit, or other purpose that violates the mission and purpose of CCA.
3. Students are prohibited from accessing materials through the Internet that may violate the moral standards, ethical beliefs, or educational philosophy of the school. This restriction includes, but is not limited to, textual, graphic and/or audio material that is:
 - Profane
 - Obscene
 - Pornographic
 - Racist
 - Violent
 - Extremist
 - Militant
 - Intimidating
 - Inappropriate

Accounts

1. Each student has a login account for access to the school's computer hardware, software, and various online resources.
2. The account is only for the use of authorized users at the school. Attempts to access the school account through any other means or from any other site is prohibited.

Network

During classroom instruction time, students must have teacher permission to navigate the Internet or use MLDs.

Email Etiquette

1. A user will log-out when finished using school computers or MLDs.
2. Email during class is prohibited unless authorized by faculty or administration.
3. Email services provided by the school are to be used only for the exchange of appropriate information.

4. Students should always use appropriate language in their email. No inappropriate email is allowed, including derogatory, obscene, or harassing messages. Email of an abusive or harassing nature is subject to disciplinary response according to the harassment and discipline policies in the CCA Parent/Student Handbook.
5. Students are prohibited from accessing anyone else's email account without first receiving explicit permission from the account holder.
6. Only the approved mail service may be used for student email.
7. School email addresses are not to be given to ANY websites, companies, or other third parties without the explicit permission of a teacher or administrator.
8. CCA reserves the right to search and read email as deemed necessary.

Passwords

Passwords are not to be shared. No one may log on to the Internet via any password other than his or her own.

Games, Social Media, Texting

1. Games are not permitted during school hours except as part of an assigned, in-class activity. Games, social media and texting are not allowed during classes, including those assigned as a Study Hall or Personalized Learning Time.
2. Screensavers that include gaming components are not allowed.

Audio and Video

1. Audio on computers should be turned off unless required for the activity being conducted in class.
2. Listening to music either aloud or with earphones is not permitted during class without the permission of the teacher.
3. The use of laptops or tablets to watch movies and videos is not permitted during class time.
4. Any audio or video recording may be conducted only with prior permission of all parties being recorded.
5. Sharing of music (including iTunes) over the school network is strictly prohibited.

Copyright

1. All information sources (textual, graphic, audio) accessible through the Internet must be cited when material is used in part, and permission must be sought and granted when material is reproduced in full. Copyright standards must comply with the copyright laws of the United States of America and/or the State of Washington.
2. Copyrighted movies may not be transferred from DVDs and placed on laptops, nor may copyrighted movies be downloaded to laptops from the Internet.
3. Plagiarism includes any use of information obtained from the Internet that is not properly cited. Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism.

Saving, Downloading & Printing

1. A student should only save data to their Google account or an alternate web-based cloud.
2. The downloading of music files, video files, etc. through the school's network is prohibited unless it is part of an assigned, in-class activity.
3. The downloading of Shareware and freeware programs such as animated cursors, screen savers, or others are strictly prohibited.

File Sharing

1. File sharing is the public or private sharing of computer data or space. Any program that creates a point-to-point connection between two or more computing devices for the purpose of sharing data is considered file sharing.
2. File sharing of any kind is prohibited both on campus and off campus. The only exception to this is when it is a specific assignment given by a faculty member.
3. No file sharing software of any kind is to be installed on school computers.

Privacy

The student's right to privacy in the school setting is not absolute. Students must expect that their computer use, files, and activity will be monitored and that the information which they create, send, receive, view, download, or store shall be subject to inspection. Student users are expected to respect the privacy of other computer users and their personal files. Student users should not reveal their personal home addresses or home telephone numbers while online.

Virus Checking & Viruses

Students who wish to use personal disks on school computers must ask the permission of the school staff. The school staff has the right to scan all disks for possible viruses. Computer users also need to be aware that viruses can come into the school's computers via the Internet or user's disks, which can then be transferred to student's personal disks. The school assumes no liability in making transfer of data available to computer users. All users take data from school computers to their personal computer systems at their own risk.

Use of School Computers

Students who have specific academic and curricular research needs have priority over students whose educational needs or wants are general or personal. Students who have exhausted other school library sources have priority over students who are using the Internet as a first stop in their research. Students who have no Internet access at their home have priority of use of the school's electronic networking over students who have outside-of-school access to the Internet. Time limits on the use of the Internet by a particular student may be established when others are waiting. Classes have priority over individuals.

Financial Obligations

1. Students may need to pay for printouts; in addition, unauthorized financial obligations resulting from inappropriate use of the Internet are the direct responsibility of the student/parent.
2. Damages to the computer hardware or software by a student will likewise result in charges being assessed against the student/parent for both parts and labor.

Liability

The student and the parent/guardian agree to absolve Concordia Christian Academy from any and all liability of any nature arising from the use of or the inability to use the computer resources at the school.

Misuse

Misuse shall include, but not be limited to, the following:

- Any attempt to bypass security systems, blocking and/or filtering software and hardware
- Opening or viewing restricted or private files
- Logging on as an administrator or as another student
- Changing system settings, altering system files or disrupting system performance
- Altering/damaging/attempting to alter or damage computer hardware or software
- Engaging in unauthorized or inappropriate use of the school's computer resources
- Ignoring instructions or directions of school staff or administration
- Abuse of, theft of, or damage to computer hardware or software
- Copying software programs, or installing software programs without approval
- Accessing, viewing, or modifying files belonging to other users without permission
- Violating copyright restrictions
- Actively or passively introducing a virus on any school computer

Mobile Learning Devices (MLDs)

1. CCA will not be held liable for any damage that may occur as a result of connecting to a CCA Wireless Network or any electrical power source.
2. CCA will not be held responsible for any physical damage, loss or theft of a student-owned mobile learning device (i.e., cell phones, tablet PCs, laptop computers, smart phones).
3. Student use of personal mobile learning devices (MLDs) in the classroom setting will be at the discretion of the classroom teacher.
4. Cell phone use in the classroom is strictly prohibited, unless authorized by the classroom teacher.

5. Illegal, destructive, harmful or other inappropriate activities - including, but not limited to, harassment of any kind as laid out in the CCA harassment policy, computer hacking, cyber-bullying, accessing offensive/obscene materials, engaging in illegal activities - are strictly prohibited.
6. Parents and/or guardians of any student bringing personal technology to school agree to be responsible for and to reimburse CCA for any damage that their student may cause by accessing the CCA wireless network with a personal MLD.
7. The text and voice features of MLDs may be utilized in a student's curriculum. The cost for these features is the sole responsibility of the student and/or guardian. CCA will not be responsible for any cost incurred from the use of MLDs in CCA curriculum or on the CCA campus.
8. Data packages (i.e., Internet access) are not required nor are they encouraged for use on student owned MLDs. Should parents/guardians choose to purchase data packages for their student's MLD or any other electronic device that accesses data outside the confines of CCA's secure and filtered network, then it is the sole responsibility of the parent to provide the filters by which the available Internet access is screened.
9. Inappropriate use of MLDs is strictly prohibited. Inappropriate use includes, but is not limited to, cheating, taking unauthorized or inappropriate pictures or videos for non-educational purposes and/or in violation of CCA's harassment or Acceptable Use Policy, using any MLD to engage in activities contrary to CCA's harassment or Acceptable Use Policy.

Violation of Acceptable Use Policy

1. CCA reserves the right to enforce appropriate consequences for the violation of any section of the Acceptable Use Policy and the Student Code of Conduct. Such consequences could include the loss of use of the computer or MLD for an amount of time determined by the administration and/or possible disciplinary action including written warnings (EDUCATE), Detention, After-Hours Work Time, suspension, dismissal, possible legal action.
2. Any violation of CCA Acceptable Use Policy may result in loss of school-provided access to electronic information. In general, the following steps will be applied, depending on severity of violation:
 - First Referral: Written (EDUCATE) warning
 - Parent, student, conference with the principal
 - Loss of technology privilege at CCA for a specified time
 - Repeated offenses or severe computer/MLD abuses may lead to more substantial consequences, including prosecution by local, state, or federal authorities.

Students are required to adhere to all provisions and conditions set forth in this Acceptable Use Policy. Students are to report any known violations of this policy to the appropriate administrative staff members.

CCA takes no responsibility for activities conducted on school computers or materials stored on school computers, laptops, or on the school's network.

CCA reserves the right to make changes or additions to the Acceptable Use Policy at any time.