CHEROKEE CHRISTIAN
IT STUDENT ACCEPTABLE USE POLICY

ACCEPTABLE USE POLICY

Cherokee Christian Schools ("CCS") provides Information Technology (IT) tools for the benefit of its staff, students, and guests. Students are responsible for good behavior on School computer networks just as they are in a classroom or a School hallway. Access to CCS IT Tools is a privilege. Without acceptance of this Acceptable Use Policy, a CCS IT Tools account will not be activated for a student.

CCS IT tools are to be used primarily to support teaching and learning. This document lays out generalized expectations for usage of these tools but can't cover every circumstance. Students and adults are expected to use good judgment when working in gray areas not covered explicitly by the rules.

Adherence to this policy shall be the joint responsibility of the students, parents, and faculty/staff of Cherokee Christian Secondary School.

BRING YOUR OWN TECHNOLOGY GUIDELINES

CCS has implemented a "bring your own device" (BYOD) program for juniors and seniors to enable students and adults to attach personal electronic devices to the School's wireless network. Students have no expectation of privacy with School-provided IT Tools and Services.

Students using privately owned electronic devices must follow the policies stated in this document while on School property, attending any School-sponsored activity, accessing School-provided resources, using the School network, or while interacting in real or delayed time with School community members. Use of these devices gives tacit approval for School IT personnel and faculty/administrators to observe and utilize the devices to confirm compliance with School policies described.

In the classroom environment, the teacher or other designated adult determines the appropriate use of technology. Teachers may declare technology-free times or call for the placing of technology at the front of the room or in a ready-to-use position. It is inappropriate to attempt to covertly use technology or overtly use technology in ways that are inappropriate, not indicated by the instructor, or that run counter to the educational purpose of the class.

Electronic devices should be used at School following guidelines that are in accord with the Word of God and which promote respect of decency, civilized behavior, and common courtesy. Use of personal or School communications tools, including but not limited to chat, telephone, e-mail, texting, or social networking should follow guidelines of Christian ethics, personal decency, and decorum. Inappropriate language, harassing behavior, overtly sexual or violent behavior, or innuendo is a violation of the letter and spirit of the rule and may be subject to disciplinary action.

Personal electronic devices should not be used in violation of any School policy or direction given by a classroom teacher or other School employee. Use of personal electronic devices for entertainment or recreational use may be severely limited by School staff, teachers or administrators based on the level of distraction and/or network resources used.

PRIVILEGES AND ACCEPTABLE USE

STUDENTS HAVE ACCESS TO:

- CCS network and internet access

- A Microsoft Office 365 account including email, calendaring, document creation, collaboration, storage, and other tools. It includes fives licenses for Microsoft Office.
- A FACTS account for LMS (Learning Management System) access
- Other classroom web resources

STUDENTS ARE ENCOURAGED TO:

- Use IT tools to support their learning in ways that are consistent with the mission of the School;
- Conduct research using the internet for instructional purposes related to class curriculum and personal interest and development;
- Access information that will facilitate their selection of the college or university that they want to attend;
- Increase their awareness of career path opportunities;
- Infuse technology into their course work;
- Improve their information literacy and research skills;
- Find ways to use technology for service to others.

CCS AND FEDERAL LAWS

Technology use in the School is governed by federal laws including the following:

Children's Online Privacy Protection Act (COPPA) COPPA limits the ability of commercial companies to collect personal information from children under 13. This permission form allows the School to act as an agent for parents in the collection of information within the School context. The School's use of student information is solely for education purposes. (http://www.ftc.gov/privacy/coppafaqs.shtm)

Family Educational Rights and Privacy Act (FERPA) FERPA protects the privacy of student education records and gives parents the rights to review student records. (http://www.ed.gov/policy/gen/guid/fpco/ferpa)

Child Internet Protection Act (CIPA) Under CIPA, CCS has measures and policies in place that protect students from harmful materials including those that are obscene and pornographic. (http://fcc.gov/cgb/consumerfacts/cipa.html)

SECURITY AND PRIVACY

Security is integral to the CCS IT network. Security guidelines for students:

- Any student identifying an IT security issue, whether on their own equipment of school-owned equipment, notify a teacher or the IT Department.
- Students may not use accounts or passwords belonging to other users.
- Attempts to gain unauthorized access to networks, equipment, or IT systems will result in cancellation of IT resource and network access.
- Students are to immediately tell their teacher or another school employee about any message they receive that is inappropriate or makes them feel uncomfortable.
- Students are responsible for their individual school accounts and should take precautions to prevent others from accessing their account. *Under no conditions* should a student share their password except to an authorized school employee.
- Parents have the right at any time to investigate the contents of their child's email and files.

UNACCEPTABLE USE

PROHIBITED ACTIVITIES:

- Using the internet or School network for any illegal activity, including gambling, computer hacking (and all variations thereof), and copyright or intellectual property law violations;

- Use of Anonymous Proxies, Caching Servers, VPN services, Proxying Browsers/Apps, or any other means to avoid restrictions placed on the IT network and/or internet access;

- Associating a website or service with the School without proper;

- Using Teams, email, or other messaging capabilities for non-school purposes;

- Posting messages on or through the network or internet, including those that are anonymous, that use abusive or profane language, or use the system to harass, insult or verbally attack others or disrupt normal function;

- Misrepresenting Cherokee Christian Schools, CCS staff members, or CCS students. Apps, sites, email, and groups are not public forums. They are extensions of classroom spaces where student free speech rights may be limited;

- Using IT tools for financial or commercial gain (unless approved by School administration for a school activity directly supervised by a staff member);

- Stealing or vandalizing data, equipment or intellectual property;

- Invading the privacy of other individuals, including:

  - copying and using the names and images of other students or faculty/staff, images of school activities, etc. on personal web pages, blogs, social media platforms, or other electronic media

  - false or derogatory online statements regarding faculty/staff or other students

  - Disclosure of personal details of faculty/staff or other students (doxxing) (such as physical addresses, phone numbers, email addresses, etc.) without express written permission.

- Attempting to gain access to or gaining access to student records, grades, or files outside of the individual authorized account;

- Use of School or personal electronic devices to perform unethical actions including, but not limited to, cheating, unauthorized collaboration, or plagiarism;

- Gaining intentional access to materials, maintaining access to materials or distributing materials which:

  - Are obscene, pornographic, or whose dominant appeal is sexual arousal;

  - Utilize or encourage excessive use of violence, blood, gore, or the diminishment of the value of life;

  - Promote academic fraud ("cheat" sites, etc.) or P2P (file-sharing) sites;

  - could be used illegally to make destructive devices such as guns, weapons, bombs, explosives or fireworks;

PROHIBITED USAGE OF SCHOOL-OWNED DEVICES:

- Downloading, installing, or accessing unauthorized software on School-owned devices without the permission of IT staff;

- Deliberately introducing a virus, spyware, malware, or any web browser extensions onto devices onto School-owned devices

PROHIBITED USAGE OF THE CCS NETWORK

- Providing access to the school's network to unauthorized individuals or granting limited authorizations to unauthorized people;

- Causing or contributing to the unnecessary congestion or malicious interference of the network;

- Attempting to gain access to or gaining access to network hardware (including wall jacks, wires, switches, routers, servers, access points, etc.) without IT permission.

- Placing unauthorized devices (routers, access points) onto the school's wired network or bridging devices on the wireless network;

PICTURES, VIDEO, AND AUDIO RECORDING:

- Taking still pictures, videos, or audio recordings of any individual, class, school event, or property (except for public events such as sporting events) without the permission of a staff member;

- Posting any such content to social media without permission;

RISKS

The educational community of the School makes no warranties of any kind, whether expressed or implied, for the service it is providing and is not responsible for any damages the user may suffer. This includes loss of data, non-deliveries, mis-deliveries, or service interruptions. The student is responsible for evaluating any information obtained from the internet. The School specifically denies any responsibility for the accuracy or quality of information obtained through its services. Additionally, the School will not be responsible for unauthorized financial obligations resulting from provided access to the internet. The users of the School's IT Tools agree that they waive any right to privacy that they may have for such use (including personal devices). School officials may monitor the user of technology and may also examine all system activities in which the user participates. Users have no right to privacy as to any information or file created, maintained, transmitted, or stored in or on School property, through our technical resources, or on personal devices at the School. Users should know that content that includes but is not limited to sexual comments or images, racial slurs or other offensive comments, defamatory, discriminatory or harassing materials distributed, accessed, or downloaded through IT tools could expose them to legal liability as well as to disciplinary action.

VIOLATIONS AND SANCTIONS

The School endeavors to create an atmosphere which fosters Christian character, academic achievement, personal responsibility, and respectful relationships among students, faculty, staff, administrators, families and other members of the School community. Any behavior or action contrary to the purposes of the School is considered an infraction and may result in the immediate and/or permanent loss of access to IT Tools and/or further disciplinary actions. At any time as required for administrative or technical reasons a network administrator may close an account.

COPYRIGHT

Cherokee Christian Schools does not sanction copyright infringement. We ask all organizations bearing the School name to honor all copyright and license restrictions.

By agreeing with this policy, I confirm that I have read and understand the following:

- Under FERPA, a student's education records are protected from disclosure to third parties. I understand that some of my student's education records stored on Schoology servers (such as student grades and assignments), PowerSchool servers (such as attendance records and permanent transcript records), and on Microsoft Office 365 (such as graded work) may be accessible to someone other than my student and Cherokee Christian Secondary School by virtue of this online environment. My signature below confirms my consent to allow my student's education records to be stored online.
- I understand that by participating in Microsoft Office 365 and Schoology, information about my child will be collected and stored electronically. I have read the privacy policies associated with use of Microsoft Office 365 (https://privacy.microsoft.com/en-us/privacystatement) and FACTS (https://factsmgt.com/privacy-policy)