CHEROKEE CHRISTIAN SCHOOLS (GRADES K-6TH) INFORMATION TECHNOLOGY AND ACCEPTABLE USE POLICY

Cherokee Christian Schools (the "School") 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. Communications on the network are often public in nature. General School rules for behavior and communications apply. Put simply, access to network services and support of those services will be provided to students who agree to act in a considerate manner.

These IT tools are to be used primarily to support teaching and learning, in accordance with the policies and guidelines contained in this document. This "Acceptable Use Policy" (AUP) addresses acceptable and unacceptable ways in which the students in our community may use our IT tools, and it addresses specific user responsibilities, rights, and expectations.

However, given the rapidly changing nature of IT systems and services, the policies defined in this document cannot cover every possible situation. Therefore, in addition to the specific acceptable and unacceptable uses presented, this AUP provides general principles which shall direct the use of the School's IT tools. 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 employees of the School. Before an IT tools account will be assigned, a student must submit this document signed by the student and the student's parent or guardian.

PRIVILEGES AND ACCEPTABLE USE

We hope that students find the School's IT tools to be useful assets that assist them in achieving their educational goals. An IT tools account grants a student access to:

- A cherokeechristian.org account (powered by Microsoft Office 365): This cloud-based computing technology grants all School students limited access to email, calendaring, document creation, collaboration, storage, and other tools.
- A PowerSchool account: This student information system gives a student access to attendance records.
- A Schoology account: This learning management system allows teachers to post assignments for students, collect completed work, provide additional learning resources, and foster an environment of collaboration.
- The internet and many subscribed internet reference and tutorial resources (which are accessible from any student computer in the building and in many cases on personal electronic devices at home and School).
- Note taking and bibliography applications
- Access to and classroom instruction on new media creation tools including music, video, digital graphics and programming software.

In ways appropriate to their grade level, users 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;

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 applies to commercial companies and limits their ability to collect personal information from children under 13. No personal student information is collected for commercial purposes by Microsoft. 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. Under FERPA, schools may disclose directory information but parents may request the School not disclose this information. Parents are provided the opportunity annually to opt out of disclosing their student's directory information on the School enrollment form. (http://www.ed.gov/policy/gen/guid/fpco/ferpa)

Child Internet Protection Act (CIPA) The School is required by CIPA to have technology measures and policies in place that protect students from harmful materials including those that are obscene and pornographic. This means that websites and student email are filtered. Mail containing harmful content from inappropriate sites will be blocked. (http://fcc.gov/cgb/consumerfacts/cipa.html)

SECURITY AND PRIVACY

Security on our IT network is a priority. Anyone identifying a security problem on the network should notify a teacher or the IT Department. If you find a problem you should not demonstrate the problem to other users or try to bypass the problem by using another individual's account.

- Users may not use accounts or passwords belonging to other users or misrepresent other users on the network.
- Unauthorized attempts to login to the network as a system administrator will result in cancellation of user privileges.
- 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 the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. *Under no conditions* should a user provide his or her password to another person except an authorized School employee.
- The School will not publish confidential education records (grades, student ID #, etc...) for public viewing on the internet. The School may publish student work and photos for public viewing but will not publish student last names or other personally identifiable information. Parents may request that photos, names and general directory information about their children not be published.
- Parents have the right at any time to investigate the contents of their child's email and files.

UNACCEPTABLE USE

The list of inappropriate uses of IT tools and accounts currently includes, but is not limited to the following. (This list may be updated at any time.)

- 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;

- Gaining intentional access to materials, maintaining access to materials or distributing materials which are obscene, pornographic, or whose dominant appeal is sexual arousal;
- Gaining intentional access to material, maintaining access to materials, or distributing materials which utilize or encourage excessive use of violence, blood, gore, or the diminishment of the value of life;
- Gaining intentional access to material, maintaining access to materials, or distributing materials which promote academic fraud ("cheat" sites, etc.) or P2P (file-sharing) sites;
- Associating a website with the School without proper authorization or representing the School by name, logo, or identity in a formal or informal publication, document, or program without prior approval;
- Downloading, installing, or accessing unauthorized software or other executable files (e.g., .exe, .bat, .pif, .reg) onto School-owned devices without the permission of IT staff; this includes but is not limited to the use of unauthorized operating systems or other root level programs that could be installed on School computers or devices.
- Deliberately introducing a virus to, or otherwise improperly tampering with, devices on the School network or the network operating system;
- Intentionally installing or accepting spyware, malware, or other disruptive, intrusive, or destructive programs;
- Attempting to gain access to or gaining access to network hardware (including wall jacks, wires, switches, routers, servers, access points, etc.). This includes placing unauthorized devices onto the School's wired network or bridging devices on the wireless network;
- Obtaining or sending information which could be used illegally to make destructive devices such as guns, weapons, bombs, explosives or fireworks;
- 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 the School, School staff members, or School students. Apps, sites, email, and groups are not public forums. They are extensions of classroom spaces where student free speech rights may be limited;
- Taking/recording still pictures, videos, or audio recordings of any individual, class, School event, or property (except for generally-public events such as sporting events) without the permission of a staff member;
- Posting audio, video, still-image, or personal information in an online environment, except when specifically authorized by a staff member;
- Posting personal contact information (full names, addresses, phone numbers, external email contact information, etc.) about themselves or other people;
- Arranging to meet someone they have met online without their parent's approval and participation;
- Using limited resources provided by the School in a wasteful manner;
- Causing or contributing to the unnecessary congestion or malicious interference of the network;
- Providing access to the School's network to unauthorized individuals or granting limited authorizations to unauthorized people;
- 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;
- Attempting to gain access to or gaining access to student records, grades, or files outside of the individual authorized account;
- Degrading or disrupting equipment or system performance;
- Failing to obey School or classroom technology use rules;

- Taking part in any activity related to technology use which creates a clear and present danger or a substantial disruption to the orderly operation of the School;
- Use of School or personal electronic devices to perform unethical actions including, but not limited to, cheating, unauthorized collaboration, or plagiarism (e.g., cell phone texting answers or taking pictures of exams).

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 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 Cherokee Christian Schools 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.

ACCEPTABLE USE POLICY - SIGNATURE

ALL PARENTS AND STUDENTS PLEASE SIGN AND RETURN THIS PAGE

By signing below, 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 current grades), PowerSchool servers (such as attendance and permanent transcript information) and on Microsoft Office 365 (such as graded work) may be accessible to someone other than my student and the 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 (http://www.microsoft.com/online/legal/v2/?docid=43&langid=en-us) and Schoology (https://www.schoology.com/privacy.php). I understand that I may ask for my child's account to be removed at any time.

Student Name: (Print) _____ Grade: _____

Student Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Please sign and return this form with the rest of the enrollment packet.