

Christian Home and Bible School

Electronic Resources Acceptable Use Policy

Text in blue is new
for 2001-2002.

for Students

Please read the following carefully before signing this document.

The term “user(s)” in this document refers to anyone who makes use of any of the electronic resources of Christian Home and Bible School (CHBS), including staff, [volunteers](#) and students. “Electronic Resources” refers primarily to computer-related devices, but also includes any other electronic device used in the school setting, such as TV, VCR, camera, audio tape device, etc.

Introduction: Christian Home and Bible School now has two full time computer labs, a mini-lab in the Media Center, and numerous other computer stations throughout campus. Most of these stations are linked together via a local area network (LAN). Furthermore, Internet access is available to both our students and our staff. Our goal is to promote innovation and educational excellence by using Internet tools for research, worldwide resource sharing, and communication.

The Internet is an electronic network of thousands of computers all over the world. Internet services provide access to electronic mail, public shareware of all types, many university and public card catalogs, and massive databases on computer networks at universities, government agencies, and private industry.

Issues: With access to computers and people all over the world also comes the availability of material that will not be considered to be of educational value in the context of the school setting. The Internet may contain material that is objectionable from many points of view. There is, however, a wealth of educational material available. Parents and guardians need to decide whether to permit their children to access the Internet.

We have taken the following measures to protect our school family from harm on the Internet.

1. Our internet access is filtered through the Bess filtering system, which provides both automatic and customizable filtering of material such as pornography, hate literature, threatening material, etc.
2. No student is to have access to the Internet without the permission and supervision of an adult staff member in the room.
3. Each student will be instructed on the dangers of the Internet and will be taught safeguards they can use to protect themselves.
4. Particularly with younger students, much of students’ Internet time will be guided; that is, teachers will “escort” them to sites that have been tested beforehand. This will not always be appropriate for older students, as a primary role of the Internet in education is that of research tool. Therefore, these students will be taught ways to avoid stumbling upon inappropriate material and what to do if such should happen.

However, **no system of protection is perfect.** On a global network **it is impossible to control access to all materials that may be considered objectionable or inappropriate.** There are those in the world who go to great lengths to camouflage their true web content, and an innocent user may stumble upon these sites from time-to-time. In addition, an industrious user may be able to gain access to sites that are believed to be filtered. Christian Home and Bible School cannot and does not guarantee that users will never have access to inappropriate or objectionable material. Parents and guardians must consider this in deciding whether to permit their children access to the Internet.

Responsibilities: The efficient, educational operation of our electronic resources relies upon the proper conduct of the users. The following guidelines are provided so that users and parents are aware of the responsibilities incurred by usage of our electronic resources, including our computers, our network, and our Internet account(s). In general, these responsibilities require ethical, efficient, courteous, and legal use of these resources. Each person having access to these resources will be made aware of what is considered acceptable and appropriate educational use.

If a user violates any of these terms and conditions, his or her access to our electronic resources, including the Internet, will be terminated and future access could be denied. The signature(s) at the end of this document is (are) legally binding and indicate(s) that the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance and agree(s) to abide by these terms.

Terms and Conditions

- 1. Acceptable Use:** Internet use must be consistent with the educational objectives of CHBS as indicated in our mission statement, our charter, our curriculum guides, and other related documents.
- A. Electronic accounts shall be used only by the authorized owner of the account and by appointed account administrators. No attempt to gain unauthorized access to such accounts is permitted. "Accounts" includes, but may not be limited to:
 - 1) user names and passwords for accessing data on a local computer, or on one or more servers on any of our Local Area Networks (LANs), or for accessing the Internet.
 - 2) network folders or other electronic file storage designations.
 - B. Unauthorized attempts to obtain access to restricted sites, servers, folders, files, databases, etc. are prohibited. This includes attempts to access other systems via any CHBS electronic resource.
 - C. Use of Internet games is forbidden, unless they are of direct educational value to a course, and are assigned and supervised by a faculty member.
 - D. Students are not permitted to use "Chat rooms", personal email or other personal messaging services unless they have direct educational value to a course, are assigned and supervised by a faculty member, and approved by the system administrator. There may be exceptions to this in special cases, such as a student needing to make contact with a parent, but even these must have staff permission and supervision.
 - E. Transmission of any material in violation of any law is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secrets.
 - F. Personal identifying information of students, such as addresses and phone numbers, shall not be made publicly available to outsiders via the CHBS Web site, except as indicated in "G" and "H", below.
 - G. Student names may be used in CHBS Web site content (sports rosters, recognition of achievement, etc.), but may not intentionally be directly connected, linked or associated with a photographic likeness of the individual student or with any other specific personal identifying information.
 - H. Photos of students may be posted on the CHBS Web site (sports photos, service clubs at work, class projects, etc.), but may not intentionally be directly connected, linked or associated with specific personal identifying information.
 - I. All passwords must be kept private. No student shall give or receive another student's password.
 - J. Internet use for personal commercial enterprise and/or financial gain is prohibited.
 - K. Students shall not be allowed to make purchases over the Internet.
 - L. No student shall be allowed to make application for any account or fill out any survey or other information-gathering form on the Internet unless such is of direct educational value to a course, and is assigned and supervised by a faculty member.

- M. Electronic vandalism is not permitted. Electronic vandalism is defined as any attempt to harm, destroy, or disrupt the data, programming or operation of another user or of another agency or network or computer station. Electronic vandalism includes, but is not limited to, the malicious uploading, downloading, or creating of computer viruses, programs, or other potentially harmful or disruptive computer instructions. It also includes the unauthorized changing of settings, properties, or configurations of any electronic resource.
- N. Computer viruses are prevalent and may cause severe damage to electronic resources. Two common ways that viruses are inadvertently transmitted are through 1) the sharing of infected removable storage media, such as floppy disks, and 2) the downloading of files from Internet sources. Antivirus software is not a foolproof safeguard. Therefore, no user shall introduce any removable storage medium (such as a floppy disk) from off campus or download files from the Internet without the permission of a knowledgeable staff member who can offer reasonable assurance that the medium or Internet source is "clean". Questionable storage media should be scanned for viruses before use. If the integrity of any storage medium or Internet source is in question, it should be avoided. CHBS understands that it will be virtually impossible to avoid virus contamination completely, but all users must exercise every reasonable caution.
- O. All users must show respect for others' privacy by safeguarding the email addresses of their email correspondents. Your correspondents can become the victims of junk email campaigns (often referred to as "spamming") if you share their email addresses with others. Do not give any person's email address to another without the permission of the address owner.
- P. Plagiarism, copyright violation, software "pirating", and theft of data via a computer or network shall not be tolerated. This includes, but is not limited to, the following areas.
1. Internet Copyright: Generally, anything on the Internet becomes copyrighted the moment it is posted. Generally, a user is in violation of this copyright the moment he/she uses such posted material without permission of the author. Some limited and temporary use of such material is considered "fair use" if a clear educational purpose can be shown, **but even in such cases, all material borrowed from the Internet should be used only with permission and should be properly credited in the work in which it is used.**
 2. Software copyright law supports the concept that consumers do not purchase ownership of software, but rather only the license to make limited use of the software. A major point of all such licenses is the limitation of the number of allowable users or installations per copy of a software title. These license agreements will be honored at CHBS. No additional, unlicensed copies or installations of software will be made.

These statements regarding copyright are not to be taken as a complete explanation of copyright law. Specific information regarding copyright regulations will be made available to students.
 3. Just as with traditional paper material, no one should attempt to use or submit another person's computer data as one's own. This includes the renaming of files and "cut/copy and paste" from one file to another.
- Q. The electronic resources of CHBS may never be used to promote, transmit or store any type of threat, harassment, or malicious prejudice against any person or group. This includes, but is not limited to, threats of violence, racial slurs, or sexually-oriented jokes or comments, etc. Harassment may include even simple, otherwise innocuous or innocent messages sent or posted in a harassing manner, such as the persistent changing of another users' screen saver message, or the posting of any message that calls undue uncomfortable attention to another person, or the posting of unflattering material which belittles another person.

2. Privileges: The use of the electronic resources at CHBS is a privilege, not a right. Inappropriate use may result in a loss of computer privileges, network/Internet access and/or user accounts, disciplinary action, and/or referral to legal authorities. The system administrators will close an account when necessary. An administrator or faculty member may request the system administrator to deny, revoke, or suspend specific user access and/or user accounts.

3. Netiquette: All users are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following: Be polite. Do not be abusive in your messages to others. Use appropriate language. Do not swear, use vulgarities or any other language inappropriate in a school setting. Carefully proofread all messages before sending/posting them. Be sure you have said what you think you have said. Avoid sarcasm; written messages do not include visual and auditory clues as to your true meaning. Your words are more likely to be taken at face value. Writing messages in all caps is the email equivalent of shouting. Use caps sparingly. Use spell check. Use proper punctuation and capitalization. Do not flood a correspondent with follow-up messages if they fail to respond as quickly as you think they should. Take heed of other netiquette suggestions that arise from time to time.

4. Limitations: CHBS makes no warranties of any kind, whether expressed or implied, for the service it is providing. CHBS will not be responsible for any damages a user suffers while on this system. These damages include loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by negligence, errors, omissions, equipment failure, or interruptions of service to the school from outside providers. Use of any information obtained via the Internet is at the user's own risk. CHBS specifically denies any responsibility for the accuracy or quality of information obtained through its electronic resources or services. All users should be aware that there are no editors of materials posted to the Internet. Anyone can post anything. Therefore, caution and wisdom should be exercised when gathering data from the Internet.

5. Security: Security is a high priority on computer networks. If users identify a security problem, they must notify the appropriate personnel immediately. Do not demonstrate the problem to other users. Do not use the Internet to discuss or disseminate information regarding security problems or how to gain unauthorized access to sites, servers, stations, files, etc.

6. Privacy: Christian Home and Bible School reserves the right to examine any materials stored or transmitted via its electronic resources. Internet users are advised that their "journeys" through the Internet can be monitored and recorded.

7. Updates: We are constantly improving our use of technology at CHBS, adding features and capabilities. Likewise, computer technology itself is in a state of rapid-fire evolution, unprecedented in any other time or industry. This is particularly true of the Internet, which seems to change before our very eyes. Therefore, this policy cannot and will not be a static document. It will be modified as our capabilities and the technologies themselves change. Users and parents will be notified of revisions and given an opportunity to renew or rescind their permission to allow students to continue to participate in the use of our electronic resources.

Christian Home and Bible School Electronic Resources Acceptable Use Policy

Student User Application/Contract

I certify that I have read the Christian Home and Bible School Electronic Resources Acceptable Use Policy (ERAUP). I understand and agree to follow the Terms and Conditions stated within that policy. I understand that any violation of the ERAUP may result in the loss of computer privileges and network/Internet access and/or my user account; may result in other disciplinary action; and may constitute a criminal offense. I agree to report any misuse of the electronic resources to school personnel. I use the Internet entirely at my own risk and I hereby release Christian Home and Bible School from any claims arising from my use of the Internet.

Note: This contract will be placed in the user's permanent file.

User Name (please print): _____

User Signature: _____ Date: ____/____/____

PARENT or GUARDIAN: As the parent or guardian of the student named above, I have read the Christian Home and Bible School Electronic Resources Acceptable Use Policy (ERAUP) and this contract. I understand that access to the Internet is designed for educational purposes. I understand that controversial material is available on the Internet and that it is not always possible to avoid it entirely. I am aware that Christian Home and Bible School has taken prudent steps to safeguard its students from such material. I will not hold Christian Home and Bible School responsible for materials my child inadvertently or deliberately accesses or acquires on the network. My child uses the Internet at his/her own risk and at my own risk. I hereby release Christian Home and Bible School from any claim arising from my child's use of the Internet. I agree to report any misuse of the school's electronic resources to a school administrator. I accept full responsibility for supervision if and when my child's use of the Internet is not in a school setting. I understand that my child's violation of the CHBS ERAUP may result in the loss of computer privileges, network/Internet access and/or my child's user account; may result in other disciplinary action; and may constitute a criminal offense. I hereby give my permission for my child to make use of the electronic resources of Christian Home and Bible School, including the accessing of Internet resources. I certify that the information contained on this application is correct.

I understand that from time-to-time my child's name may appear on the Christian Home and Bible School Web site, but that it will not intentionally be directly connected, linked or associated with a photographic likeness of my child or with any other specific personal identifying information.

I understand that from time-to-time my child's photographic likeness may appear on the Christian Home and Bible School Web site, but that it will not intentionally be directly connected, linked or associated with my child's name or with any other specific personal identifying information.

Parent or Guardian Name (please print): _____

Signature: _____ Date: ____/____/____