

CASTLE HILLS FIRST BAPTIST SCHOOL

Acceptable Use Policy for School Technology Resources

Please Read, Sign and Return with Completed Application

PURPOSE:

Castle Hills First Baptist School provides Technology Resources to its users (students and staff) for educational and administrative purposes. Technology Resources include the intranet, Internet access, fax, E-mail, stand-alone computer, and telephone. The goal in providing these resources is to promote educational excellence in Castle Hills First Baptist School by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers, and support staff. The use of these Technology Resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in context of the school setting. Castle Hills First Baptist School firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the school.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Castle Hills First Baptist School activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage.

The privilege of using the Technology Resources is attended by the responsibility to use the resources properly. Accordingly, policies have been developed to ensure that the technology equipment is well maintained so that the users have uninterrupted access. These policies are not designed to restrict students in the use of technology. They are designed to give students guidelines in the proper use of the Technology Resources so there is little down time.

Our enthusiasm for the opportunities electronic resources has created has not in any way lessened the commitment to making sure that these resources are used for purposes related to the educational mission of Castle Hills First Baptist School. Accordingly, the purpose of all Internet and other electronic resources is to support the school's mission. Consequently, student use of these resources must be for matters directly related to one's academic or approved extra-curricular obligations at CHFBS. Conduct on the computers is to reflect and be consistent with Christian ethical and moral principles, and precepts, consistent with the high standards of character and conduct expected of all students and faculty and is in compliance with all school policies. We have established the following policies to make sure these resources are used appropriately:

1. The faculty will monitor the lab.
2. Acceptable Use Policies are clearly posted in the lab.
3. Within the CHFBS network anonymity is not allowed.
4. Users of Technology Resources may not:
 - a) Attempt to gain unauthorized access to any other computer system (to log in through another person's account or access another person's files, even if only for the purposes of "browsing", "snooping", or "electronic discovery")
 - b) Make connections that allow unauthorized access to Castle Hills First Baptist School's network
 - c) Deliberately disrupt or harm hardware or systems

- d) Create a danger of service disruption
 - e) Interfere with computer performance
 - f) Interfere with another's ability to use equipment and systems
 - g) Destroy data.
 - h) Seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users
5. Users of Technology Resources may not:
- a) Use, forward or post personal information on the Internet about themselves or other people
 - b) Agree to meet with someone they have met on the Internet
 - c) Use, forward or post any personal contact information (i.e. address, telephone, school address, work address, pictures or video bites, and clips)
 - d) Use, forward or post information that could knowingly or recklessly:
 - i) endanger an individual
 - ii) cause personal damage
 - iii) be false or defamatory about a person or organization.
 - e) Use, forward or post obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening, or disrespectful language
 - f) Engage in personal attacks, including prejudicial or discriminatory attacks
 - g) Harass another person (persistently acting in a manner that distresses or annoys another person)
 - h) Use, forward or post chain letters or engage in "spamming" (sending an annoying or unnecessary message to a large number of people)
 - i) Use, forward or post material in violation of local, state, or federal laws
 - j) Use, forward or post copyrighted or material covered by trade secret.
6. Users of Technology Resources may not:
- a) Trade any products or services that are not affiliated with School business
 - b) Buy, sell, or advertise
 - c) Engage in illegal acts
 - d) Plagiarize works that they find on the Internet or other resources.
 - e) Use Technology Resources:
 - i) for personal gain
 - ii) for private business activities
 - iii) for unauthorized personal use
 - iv) for any commercial activities
 - v) for any political lobbying
 - vi) for tasks that are unrelated to students' academic or extra-curricular obligations
7. Users may not access, download, install, store or reproduce software on a school computer:
- a) Without the approval of appropriate school personnel
 - b) That is profane or obscene (pornography of any kind)
 - c) That advocates illegal acts
 - d) That advocates violence or discrimination towards other people (hate literature).
8. Students are:
- a) To use the computer labs whenever possible
 - b) To ask for help in using the computers
 - c) To ask for help in conducting on-line research
 - d) To return all CD's, books, and computer disks
 - e) To treat the equipment with care

- f) To enjoy the lab
- 9. Students are not permitted:
 - a) In the computer lab without approved adult supervision
 - b) To bring food or drink into the computer lab at anytime
 - c) To install computer programs, including games
 - d) To delete programs
 - e) To change the computer color schemes or the desktop arrangement
 - f) To exit to the DOS prompt to list or manipulate file directories or to run programs
 - g) To change any system configurations
 - h) To remove CD's, books, or computer disks from the lab
 - i) To rename any computer files
 - j) To move program or document files
 - k) To change, move, or otherwise tamper with computer hardware or network connections

SYSTEM SECURITY OBLIGATIONS

Users are responsible for the use of their individual access account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his/her password to another person.

Attempts to log on to Castle Hills First Baptist School's private network or any other network as a system administrator is prohibited. Any user identified as a security risk or having a history of violating this or any other Castle Hills First Baptist School policies may be denied access to Castle Hills First Baptist School's private network. Users should immediately notify a teacher or system administrator of any possible security problem.

Students will promptly disclose to their teacher or other appropriate school employee any message or information received that is inappropriate.

Use of all School Technology Resources is subject to review, access, and monitoring, even if a private password or other private access code is used. Any use of School Technology Resources such as telephones, Internet, e-mail, or other resources is not private and users should have no expectation of privacy when using such resources for personal use.

FILTERING

As required by law and in recognition of the need to establish a safe and appropriate computing environment, Castle Hills First Baptist School will use filtering technology to prohibit access, to the degree possible, to objectionable or unsuitable content that might otherwise be accessible via the Internet.

SUPERVISION AND ENFORCEMENT

The Superintendent has the responsibility to establish a system to ensure adequate:

1. Interpretation and enforcement of all Technology Resource Policies
2. Supervision of students using the Technology Resources
3. Maintenance of executed user agreements for all users

The Superintendent has the responsibility to interpret and enforce this policy for employees including maintaining executed user agreements.

Castle Hills First Baptist School will cooperate with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through Castle Hills First Baptist School's private network.

INTERNET

The Internet may be accessible to users. The School has the right to place reasonable restrictions on the material accessed or posted throughout its system.

Castle Hills First Baptist School may provide Internet access to users as a means to facilitate resource sharing, innovation, and communication. Information gathered from the Internet is viewed in the same manner as other reference material in the school. Such resources enhance the learning environment.

School personnel provide guidance to the student in Internet use and monitor the program to the best of their ability as a regular instructional activity. Controlling all materials on a global network is impossible, and a user may discover inappropriate information or perform inappropriate actions in spite of adult supervision. Therefore, we encourage parents to have a frank discussion with their children about biblical Christian values and how those beliefs should guide student activities while using the Internet.

School personnel will:

1. Teach proper techniques and standards for Internet participation.
2. Guide student access to appropriate areas of Internet.
3. Assure that students understand that misuses of the Internet could result in loss of access privileges or other privileges.

STUDENT ACKNOWLEDGMENT AND PARENT OR GUARDIAN CONSENT FOR STUDENT USE OF THE CASTLE HILLS FIRST BAPTIST SCHOOL TECHNOLOGY RESOURCES

The student and parent/guardian must sign the Acceptable Use Policy for School Technology Resources Agreement Form before the student is given access to the school's Technology Resources. School personnel or the parent/guardian may withdraw student technology access at any time.

The parent/guardian is responsible for any damage caused by the student's inappropriate use of the School's Technology Resources.

CASTLE HILLS FIRST BAPTIST SCHOOL
ACCEPTABLE USE POLICY FOR SCHOOL TECHNOLOGY RESOURCES
AGREEMENT FORM

This form must be signed and returned with the completed application packet.

(NOTE: Students will not be permitted to use the lab until this form is signed and returned)

I have read the Acceptable Use Policy for School Technology Resources. I have discussed them with my child. In consideration of the privilege of my child using the school's Technology Resources, and in consideration of having access to the public networks, I hereby release Castle Hills First Baptist School, their operators, administrators, faculty, staff, and employees from any and all claims and damages of any nature arising from my child's use of, or inability to use, the School's Technology Resources, including, without limitation, the types of damage identified in the Acceptable Use Policy for School Technology Resources.

I give permission for my child, _____, to use the Technology Resources including the Internet, and certify that the information contained on this form is correct.

Parent's Signature

Date

I have read the school's policies regarding the use of the school's Technologies Resources. **I pledge my honor** to adhere to these policies, and I understand that violation of these policies is an honor offense and will lead to disciplinary action, including the possible loss of computer lab privileges.

Student's Signature

Date

Grade

Student's Signature

Date

Grade

Student's Signature

Date

Grade