CHRISTIAN CHAPEL ACADEMY
Technology Use Policy
Revised: 10-11-06

The use of any Christian Chapel Academy computer is a privilege, not a right. Users of computers are obligated to conform to CCA policies and directions given by a staff member. Using the CCA facilities to access information carried by the Internet or other such information services must be for academic work assigned by a teacher. Depending on the nature of the situation, students who violate this regulation shall be subject to disciplinary action, or as the case is with any other property of CCA, be held responsible for the cost of repair or replacement of any damaged equipment or materials.

Technology Usage: Christian Chapel Academy recognizes the educational and professional value of electronics-based information technology, both as a means of access to enriching information and as a tool to develop skills that students need. The school's technology exists for maximizing the educational opportunities and achievement of CCA students. The network is considered a limited purpose device. The professional enrichment of the staff and increased engagement of the students' families and other patrons of the school are assisted by technology, but are secondary to the ultimate goal of student achievement. Use of technology resources in a disruptive, manifestly inappropriate or illegal manner impairs the school's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to the school's technology resources. Development of students' personal responsibility is itself an expected benefit of the school technology program.

Definitions: For the purposes of this policy and related regulation, procedures and forms, the following terms are defined:
User- any person who is permitted by the school to utilize any portion of CCA's technology resources, including but not limited to students, employees, church members and agents of the school or church.
User Identification (ID) - any identifier that would allow a user access to the school's technology resources, or to any program, including but not limited to, e-mail and Internet access.
Password- a unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

User Identification and Network Security: CCA technology resources may be used by authorized students, employees, patrons and other persons such as consultants, legal counsel and independent contractors. Use of the school's technology resources is a privilege, not a right. No student, employee, or other potential user will be given an ID, password or other access to school technology if he/she is considered a security risk by the Principal or designee.
Users must adhere to school policies, regulations, procedures, and other school guidelines. All users shall immediately report any security problems or misuse of the school's technology resources to an administrator or teacher.

User Agreement: Unless authorized by the Principal or designee, all users must have an appropriately signed *User Agreement* on file with the school before they are allowed access to CCA technology resources. All users must agree to follow the school's policies, regulations and procedures. In addition, all users must recognize that they do not have a legal expectation of privacy in any e-mail use activities involving the school's technology. A user ID with e-mail access, if granted, is provided to users of this school's network and technology resources only on condition that the users consents to interception or access to all communications accessed, sent, received or stored using CCA technology in his or her *User Agreement*.

Content Filtering and Monitoring: CCA will monitor the on-line activities of minors and operate a technology protection measure ("filtering/blocking device") on all computers with Internet access. The filtering/blocking device will attempt to protect against access to visual depictions that are obscene, harmful to minors, and pornography. Because the school's technology is a shared resource, the filtering/blocking device installed by the school, including attempts to evade or disable, is a serious violation of school policy.

Closed Forum: CCA's technology resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law.
The school's web page will provide information about the school, but will not be used as an open forum. Any expressive activity involving school technology resources that students, parents and members of the public might reasonably perceive to bear the imprimatur of the school, and which are designed to impart particular knowledge or skills to student participants and audiences, are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school for legitimate pedagogical reasons. All other expressive activity involving the school's technology is subject to reasonable prior restraint and subject matter restrictions as allowed by law and school policies.

Student Users: No student will be given access to the school's technology resources until the school receives a *User Agreement* signed by the student and the student's parent(s), guardian(s), or person(s) standing in the place of a parent. Students who are 18 or who are otherwise able to enter into an enforceable contract may sign the *User Agreement* without additional signatures. The Principal or designee in unusual situations may grant students who do not have a User Agreement on file with the school permission to use school technology.

Privacy: A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the school's technology resources. All CCA technology resources are considered school property. The school may maintain or improve technology resources at any time. The school may remove, change or exchange hardware or other technology between classrooms, employees, students or any other user at any time, without prior notice. Authorized CCA personnel may load or delete new programs or information, install new equipment, upgrade any system or enter any system to correct problems at any time. CCA may examine all information stored on school technology resources at any time. The school may monitor employee and student technology usage. Electronic communications, all data stored on the school's technology resources, and download material, including files deleted from a user's account, may be intercepted, accessed or searched by school administrators or designees at any time.

Violations of Technology Usage Policies and Procedures: Use of CCA's technology resources is a privilege, not a right. A user's privileges may be suspended pending an investigation concerning use of the school's technology resources. Any violation of school policy, regulations or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. The administration may use disciplinary measures to enforce school policy, regulations and procedures. Students may be suspended or expelled for violating CCA's policies, regulations and procedures. Employees may be disciplined or terminated for violating the school's policies, regulations and procedures. Any attempted violation of school policy, regulations or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Sanctions:
1. Violations may result in a loss of access.
2. Additional disciplinary action may be determined in line with existing practice regarding inappropriate language or behavior.
3. When applicable, law enforcement agencies may be involved.

Damages:
All damages incurred by CCA due to the misuse of the school's technology resources, including the loss of property and staff time, will be charged to the user. School administrators have the authority to sign any criminal complaint regarding damage to school technology.

General Rules and Responsibilities:
All users of CCA's technology resources will comply with the following rules and responsibilities.

1. Applying for a user ID under false pretenses is prohibited.
2. Using another person's user ID and/or password is prohibited.
3. Sharing one's user ID and/or password with any other person is prohibited.
4. A user will be responsible for actions taken by any person using the ID or password assigned to the user.
5. Deletion, examination, copying or modification of files and/or data belonging to other users without their prior consent is prohibited.
6. Mass consumption of technology resources that inhibits use by others is prohibited.
7. Non-educational Internet usage is prohibited except for reasonable, incidental personal purposes.
8. Use of school technology for soliciting, advertising, fund-raising, commercial purposes or for financial gain is prohibited, unless authorized by the school.
9. Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
10. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The school will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using school technology in violation of any law.
11. Accessing, viewing or disseminating information using school resources, including e-mail or Internet access, that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, pervasively indecent or vulgar, or advertising any product or service not permitted to minors is prohibited.
12. Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of school staff for curriculum-related purposes.
13. Accessing, viewing or disseminating information using school resources, including e-mail or Internet access, that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g. threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful school regulations is prohibited.
14. Any use which has the purpose or effect of discriminating or harassing any person or persons on the basis of race, color, religion, sex, national origin, ancestry, disability, age, pregnancy, or use of leave protected by the Family and Medical Leave Act or the violation of any person's rights under applicable laws is prohibited.
15. Any unauthorized, deliberate, or negligent action, which damages or disrupts technology, alters its normal performance, or causes it to malfunction, is prohibited, regardless of the location or the duration of the disruption.
16. Users may only install and use properly licensed software, audio or video media approved for the use by the school. All users will adhere to the limitations of the school's technology licenses. Copying for home use is prohibited unless permitted by the school's license, and approved by the school.
17. At no time will school technology or software be removed from the school premises, unless authorized by the school.
18. All users will use CCA's property as it was intended. Technology or technology hardware will not be lifted, moved or relocated without permission from an administrator. All users will be held accountable for any damage they cause to school technology resources.
19. All damages incurred due to the misuse of the school's technology will be charged to the user. CCA will hold all users accountable for the damage incurred and will seek both criminal and civil remedies, as necessary.

20. Electronic resources provided for home access are for the exclusive use of CCA students and staff.
21. Web pages by teachers shall be hosted on servers maintained by the school or on an approved site. All school web pages including teacher web pages shall be approved prior to posting. Content of web pages hosted on school web sites need to be education or school focused.

Technology Security and Unauthorized Access:
All users shall immediately report any security problems or misuse of the school's technology resources to a teacher or administrator. No person will be given access to CCA technology if he/she is considered a security risk by the Principal or designee.

1. Use of CCA technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.
2. Use of CCA technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
3. The unauthorized copying of system files is prohibited.
4. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any school technology are prohibited.
5. Any attempts to secure a higher level of privilege on the technology resources without authorization are prohibited.
6. The introduction of the computer "viruses," "hacking" tools, or other disruptive/destructive programs into a school computer, the school network, or any external networks are prohibited.

On-line Safety ~ Disclosure, Use, and Dissemination of Personal Information:

1. All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.
2. Student users are prohibited from sharing personal information about themselves or others over the Internet, unless authorized by the school.
3. Student users shall not agree to meet with someone they have met on-line without parental approval.
4. A student user shall promptly disclose to his/her teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.
5. Users shall receive or transmit communications using only CCA-approved and school-managed communication systems. For example, users may not use messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by CCA.
6. All CCA employees will abide by state and federal law and Church policies and rules when communicating information about personally identifiable students.
7. Employees shall not transmit confidential student information using school technology, unless designated for that use. Employees will take precautions to prevent negligent disclosure of student information or student records.
8. No curricular or non-curricular publication distributed using school technology will include the address, phone number or e-mail address of any student without permission.

Electronic Mail: A user is responsible for all electronic mail ("e-mail") originating from the user's ID or password.

1. Forgery or attempted forgery of e-mail messages is illegal and prohibited.
2. Unauthorized attempts to read, delete, copy or modify the e-mail of other users are prohibited.
3. Users are prohibited from sending unreasonable amounts of unsolicited electronic mail unless the communication is a necessary, employment-related function, or an authorized publication.
4. All users must adhere to the same standards for communicating on-line that are expected in the classroom, and consistent with the school policies, regulations and procedures.

Exceptions
Exceptions to school rules will be made for CCA employees or agents conducting an investigation of a use, which potentially violates the law, school policy, regulations or procedures. Exceptions will also be made for technology administrators who need access to school technology resources to maintain the school's resources or examine and delete data stored on school computers as allowed by CCA's retention policy.

Waiver
Any user who believes he/she has a legitimate reason for using CCA's technology in a manner which may violate any of the school's adopted policies, regulations and procedures may request a waiver from the Principal or designees. In making the decision to grant a waiver to a student, the administration shall consider the purpose, age, maturity, and level of supervision involved.

No warranty/No Endorsement
CCA makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The school's technology resources are available on an "as is, as available" basis.

CCA is not responsible for loss of data, delays, non-deliveries, mis-deliveries or service interruptions. The school does not guarantee the accuracy or quality of information obtained from the Internet, or use of its technology resources. Access does not include endorsement of content or the accuracy of the information obtained.

CHRISTIAN CHAPEL ACADEMY

Student Name _____ Student ID Number _____

Technology Authorization & Usage Policy Form

Computer/Technology Usage Policy: *(Kindergarten-grade 8)*
I understand that a copy of the Christian Chapel Academy Technology Usage policy is available on the school website (www.christianchapel.us/cca) or in the school office. I have read and discussed this policy with my student regarding safe and responsible technology usage. My student has agreed to abide by the school technology usage policy.

_____ Yes, my student can use the computers on the Christian Chapel Academy network.
_____ No, my student cannot use the computers on the Christian Chapel Academy network.

Email Permission: *(Grades 6-8)*
I grant permission for him/her to have access to electronic mail. My student has agreed to abide by the CCA technology usage policy. I also understand the purpose of this e-mail is to further educational goals and objectives.

_____ Yes, my student may have an e-mail account.
_____ No, my student may not have an e-mail account.

Wireless Usage: *(Grades 6-8)*
I understand that any wireless device brought to school by my child must comply with all existing technology policies and procedures in effect for Christian Chapel Academy. I also understand that any device lost, damaged or stolen at school is not the responsibility of the Christian Chapel Academy.

_____ Yes, I agree to the policy for wireless devices.
_____ No, I do not agree to the policy for wireless devices.

Media Waiver & Release: *(ALL students)*
I consent to my child being photographed, interviewed and/or videotaped by representatives of Christian Chapel Academy /media outlets (newspaper, T.V. stations, etc.). Any information or images obtained from those activities may be reproduced by the school and/or the public media for use in advertising, publicity or educational activities, including but not limited to school publications, videos, print and television news. I hereby waive any claims I may have, and release the school and its employees from liability of claims arising out of such activities.

_____ Yes, my child may be photographed, interviewed or videotaped for media use.
_____ No, my child may not be photographed, interviewed or videotaped for media use.

Christian Chapel Academy Website: *(ALL students)*
I consent to my student's name and/or picture appearing on the school's website.

_____ Yes, I do. _____ No, I do not.

Verification:
I verify that the information provided on this form is accurate and current, and that I am the legal parent/guardian of the student.

X_____ _____ _____
SIGNATURE of Parent/Guardian PRINT Name of Parent Date