

CATHEDRAL HIGH SCHOOL

Student Acceptable Use Policy and Internet Safety Guidelines 2008-09

Cathedral High School (CHS) is pleased to make available to students access to interconnected computer systems within the school's local area network and to the internet, the worldwide network that provides various means of accessing significant educational materials and opportunities.

In order for CHS to be able to continue to make its computer network and internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and internet access may jeopardize the ability of all students to enjoy such access. While the school's teachers and other staff will make reasonable efforts to supervise student use of the network and internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Below is the Acceptable Use and Internet Safety Policy ("Policy") of CHS and the Internet Service Provider that provides internet access to CHS. Upon reviewing, signing, and returning this Policy as the students have been directed, each student will be given the opportunity to enjoy internet access at CHS and is agreeing to follow this Policy. If a student is under 18 years of age, he or she must have his or her parent or guardian read and sign the Policy. CHS cannot provide access to any student who, if 18 years of age or older, fails to sign and submit the Policy to the school as directed or, if under the age of 18, does not return the Policy as directed with the signatures of the student and his/her parent or guardian.

Listed below are the provisions of your agreement regarding computer network and internet use. If you have any questions about these provisions, you should contact the Technology Coordinator. If any user violates this Policy, the student's access will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action.

I. PERSONAL RESPONSIBILITY

By signing this Policy, you are agreeing not only to follow the rules in this Policy but also to report any misuse of the network to the Technology Coordinator. Misuse means any violations of this Policy or any other use that is not included in the Policy but has the effect of harming another or his or her property.

II. TERM OF THE PERMITTED USE

A student who submits to the school, as directed, a properly signed Policy and follows the Policy to which he or she has agreed, will have computer network and internet access during the course of the school year only. Students will be asked to sign a new Policy each year during which they are students at CHS before they are given an access account.

III. ACCEPTABLE USES

A. Educational Purposes Only

CHS is providing access to its computer networks and internet for only educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the Technology Coordinator to help you decide if a use is appropriate.

IV. ACCEPTABLE USE AND INTERNET SAFETY POLICY

Acceptable Use

The purpose of the internet is to facilitate communications in support of research and education by providing access to unique resources and an opportunity for collaborative work.¹ To remain eligible as a user, the use of the account must be in support of and consistent with the school's educational objectives.

Privilege

The use of the internet is a privilege, not a right. Inappropriate use, including any violation of these condition and rules, may result in the cancellation of this privilege.

A. Responsible User

A responsible user of the school network and internet may keep an account as long as the user is a student at CHS. A responsible user may:

- use the internet to research assigned classroom projects
- use the internet to send email² to other users only when corresponding on school projects.

¹ The network is considered a limited forum, similar to a school newspaper, and therefore CHS may restrict your speech for valid educational reasons. The school will not restrict your speech on the basis of a disagreement with the opinions you are expressing. You may not use the network for political lobbying. But you may use the network to communicate with elected representatives and to express your opinion on political issues.

² Cathedral High School provides each student with an email account for educational uses only. You must not let anyone else use your account. You are responsible for all activities that originate from your email account. (If you suspect that your password has been compromised, ask the Technology Coordinator to change it for you immediately.) Be aware that messages are blocked for inappropriate language. Messages sent to or received from sources outside of the school community are also blocked and checked by a staff email administrator to confirm educational purpose and to assure appropriateness, thereby further securing the safety of students. For this reason, **use of outside email accounts (such as yahoo, google, or AOL, for example) is strictly forbidden.** Because school email accounts will be used for important announcements and updates, as well as for communications with classroom teachers, students are responsible for activating their school accounts and checking email on a regular basis.

- use the internet to explore other computer systems

A responsible user:

- may NOT use the internet for any illegal purpose
- may NOT use instant messaging
- may NOT sign onto social networks (e.g. myspace.com, facebook.com, etc.)
- may NOT randomly search the internet without a teacher's express consent
- may NOT download images, files or music without a teacher's express consent
- may NOT participate in or generate hate mail
- may NOT use the network to access obscene or pornographic material
- may NOT use impolite or abusive language
- may NOT violate the rules of common sense of etiquette
- may NOT change or edit computer files that do not belong to the user
- may NOT receive copyrighted material without permission

Note that system administrators have access to all user accounts, files, etc. including email.

By signing this agreement, you acknowledge that you:

- understand the rules and regulations of CHS's Acceptable Use Policy
- realize that if the rules are violated your privileges will end.
- understand that there will be no second chances.

B. Unacceptable Uses of the Network

Among the uses that are considered unacceptable and which constitute a violation of this Policy are the following:

1. Uses that violate the law or encourage others to violate the law. Don't transmit offensive or harassing messages; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them.
2. Uses that cause harm to others or damage to their property. For example, don't engage in defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the internet; upload a worm virus, "Trojan horse," "time bomb" or other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.

3. Uses that jeopardize the security of student access and of the computer network or other networks on the internet. For example, don't disclose or share your password with others; don't impersonate another user.³
4. Uses that are commercial transactions. Students and other users may not sell or buy anything over the internet. You should not give others private information about you or others, including credit card numbers and social security numbers.

C. Netiquette

All users must abide by rules of network etiquette, which include the following:

- Be polite. Use appropriate language: no swearing, vulgarities, suggestive, obscene, belligerent or threatening language.
- Avoid language and uses that may be offensive to other users. Don't use access to make, distribute, or redistribute jokes, stories, or other material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
- Don't assume that a sender of email is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her email address to third parties. This should only be done with permission or when you know that the individual would have no objection.
- Be considerate when sending attachments with email (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format that the recipient can open.

V. INTERNET SAFETY

A. *General Warning--Individual Responsibility of Parents and Users.* All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and internet and stay away from these sites. Parents of minors are the best guides to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the Technology Coordinator.

B. *Personal Safety.* Be safe. In using the computer network and internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name, or any other information, which might allow a person to locate you without first obtaining the

³ You are responsible for the security of your password and your individual account; therefore, you should take all reasonable precautions to prevent others from being able to use your account. Under no conditions should you provide your password to another person. Choose a password that cannot be easily guessed. The best passwords are 6-8 characters long and include a mixture of lower case letters, upper case letters, numbers and characters (e.g. @, &, *). See the network administrator if you need to change your password or suspect that it has been compromised.

permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you “meet” on the computer network or internet without your parent’s permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the internet in a secluded place or in a private setting.

C. *“Hacking” and Other Illegal Activities.* It is a violation of this Policy to use the school’s computer network or the internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

D. *Confidentiality of Student Information.* Personally identifiable information concerning students may not be disclosed or used in any way on the internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the internet, particularly credit card numbers and social security numbers.

E. *Active Restriction Measures.* CHS, either by itself or in combination with the Data Acquisition Site providing internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are 1) obscene, 2) child pornography, or 3) harmful to minors. CHS will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material, which is inappropriate for minors.⁴

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 or older.

VI. PRIVACY

Network and internet access is provided as a tool for your education. CHS reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the computer network and internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of CHS, and no user shall have any expectation of privacy regarding such materials.

⁴ Cathedral High School subscribes to a content filter, which identifies and prohibits access to sites deemed inappropriate for educational users. No system is perfect, however, so users must take responsibility for their own actions and take steps to safeguard themselves. Subscription to the content filter is a requirement of the Children’s Internet Protection Act (CIPA). Use of proxy servers (sometimes called “myspace proxies”) to by-pass the content filter in order to access web sites blocked by the filter (e.g. Myspace) is a serious violation of this policy, as it willfully circumvents a provision required by CIPA. The content filter blocks many of these proxy sites, but many more are created daily and are not blocked. It is impossible to block all of them, so students must take the responsibility to avoid using these to intentionally visit blocked sites.

VII. FAILURE TO FOLLOW POLICY

The user's use of the computer network and internet is a privilege, not a right. A user who violates this Policy shall, at a minimum, have his or her access to the computer network and internet terminated, which CHS may refuse to reinstate for the remainder of the student's enrollment in CHS. A user violates this Policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this Policy if he or she permits another to use his or her account or password to access the computer network and internet, including any user whose access has been denied or terminated. CHS may also take other disciplinary action in such circumstances.⁵

VIII. WARRANTIES/INDEMNIFICATION

CHS makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the internet provided under this Policy. It shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the internet under this Policy. By signing this Policy, users are taking full responsibility for his or her use, and the user who is 18 or older or, in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold CHS, the Internet Service Provider that provides the computer and internet access opportunity to CHS, and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from the user's access to its computer network and the internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the School in the event of the School's initiating an investigation of the user's use of his or her

⁵ Routine maintenance and monitoring of the network may lead to discovery that you have violated this Policy, the student handbook, or the law. The School will monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material that is inappropriate for minors. An individual search will be conducted if there is reasonable suspicion that you have violated this Policy, the student handbook, or the law. The investigation will be reasonable and related to the suspected violation. Your parents have the right at any time to request to see the contents of your files.

The school will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the network. In the event there is a claim that you have violated these regulations or the student handbook in your use of the network, you will be provided with notice and an opportunity to be heard in the manner set forth in the student handbook. If the violation also involves a violation of other provisions of the student handbook, it will be handled in a manner described in the student handbook. Additional restrictions may be placed on your use of your Internet account.

access to its computer network and the internet, whether that use is on a School computer or on another computer outside CHS's network.

IX. UPDATES

Users, and if appropriate, the user's parents/guardians, may be asked from time to time to provide new or additional registration and account information or to sign a new Policy, for example, to reflect developments in the law or technology. Such information must be provided by the user (or his/her parents or guardian) or such new Policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the Technology Coordinator.

CATHEDRAL HIGH SCHOOL STUDENT ACCOUNT AGREEMENT 2008-09

Student Section

(to be read and signed by every student, regardless of age)

Student Name (print clearly) _____ Grade _____

I have read, understood and agree to abide by the terms of the foregoing Acceptable Use Policy and Internet Safety Policy. Should I commit any violation or in any way misuse my access to Cathedral High School's computer network and the internet, I understand and agree that my access privilege may be revoked and school disciplinary action may be taken against me. Refer to the Student Handbook for details about consequences for violating this policy.

Student Signature _____ Date _____

User (place an "X" in the correct blank): I am 18 or older _____ I am under 18 _____

If I am signing this policy when I am under 18, I understand that when I turn 18, this Policy will continue to be in full force and effect and agree to abide by this Policy.

Parent or Guardian Section

(to be read and signed by parents/guardians of students who are under 18).

As the parent or legal guardian of the above student, I have read, understand, and agree that my child or ward shall comply with the terms of Cathedral High School's Acceptable Use and Internet Safety Policy for the student's access to enter Cathedral High School's computer network and the internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the school to restrict access to all offensive and controversial materials and understand my child's or ward's responsibility for abiding by the Policy.

I am therefore signing this Policy and agree to indemnify and hold harmless Cathedral High School and the internet service provider against all claims, damages, losses, and costs, of whatever kind, that may result from my child's or ward's use of his or her access to such networks or his or her violation of the foregoing Policy. Further, I accept the responsibility for supervision of my child's or ward's use of his or her access account if and when such access is not in the school setting. I hereby give permission for my child or ward to use the building-approved account to access Cathedral High School's computer network and internet.

Parent or Guardian Signature _____ Date _____

Parent or Guardian Name (print clearly) _____ Phone _____

Street Address _____ City, State _____ Zip Code _____