

FOR THOSE USING CHCA'S COMPUTER NETWORK AND ACCESSING INTERNET THROUGH THE SCHOOL

Cincinnati Hills Christian Academy ("CHCA") offers access to its students, faculty, staff, administrators or anyone else authorized to use the CHCA resources to interconnected computer systems within CHCA and to the Internet (via school devices and personal devices), which provides both various means of accessing significant educational materials and opportunities and is an excellent research tool for life-long learning. CHCA has established parameters for this use in the spirit of the Christian mission and CHCA's core values.

So that CHCA can continue to make its computer network and Internet access available, all students, faculty, staff, administrators or anyone else authorized to use the CHCA resources, must take responsibility for appropriate and lawful use of this access. In particular, students must understand that one student's misuse of the network and Internet access may jeopardize all other students' ability to enjoy such access. While CHCA's teachers and other staff will make reasonable efforts to supervise student use of network and Internet access, student cooperation is critical in exercising and promoting responsible use of this access.

Below is CHCA's Responsible Use and Internet Safety Policy ("Policy") and the Data Acquisition Site that provides Internet access to CHCA. Upon the parents'/legal guardians' reviewing and agreeing to this Policy as part of executing the CHCA Enrollment Contract, each student is bound by the Policy and will be given the opportunity to enjoy Internet access at School. CHCA cannot provide access to any student who, if 18 or older, fails to sign and submit the Policy to CHCA as part of executing the CHCA Enrollment Contract.

Listed below are the provisions of your agreement regarding computer network and Internet use. This policy also applies to use of personal devices on a non-school data network while on school property, at a school event or while participating in a school activity such as remote or online learning. Please contact the Director of Academics and/or the appropriate Division Administrator (principal, assistant principal) with any questions about these provisions. If any user violates this Policy, the student will be subject to disciplinary action, including denial of access to the network and/or school devices, or other consequences as deemed appropriate by the school administration.

I. PERSONAL RESPONSIBILITY

By signing your CHCA Enrollment Contract, you have agreed not only to follow the rules in this Policy, but are agreeing to report any misuse of the network to the Director of Academics and/or the appropriate Division Administrator (principal, assistant principal). Misuse means any violations of this Policy or any other use that is not included in the Policy, but can harm others or their property.

II. TERMS OF THE PERMITTED USE

Students who are enrolled are permitted to have computer network and Internet access while they are actively taking courses only.

III. ACCEPTABLE USES

Educational Purposes Only. CHCA provides equipment and access to its computer networks, the Internet and its online resources for educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the Director of Academics and/or the appropriate division administration to help you decide if a use is appropriate.

IV. UNACCEPTABLE USES

A. Some unacceptable uses that violate this Policy are:

1. Uses that violate the law or encourage others to violate the law. Don't transmit offensive or harassing messages; offer for sale or use any substance, the possession or use of which is prohibited by CHCA's Student Discipline Policy; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; or 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. This includes any live or recorded classes, whether in person or virtual, that CHCA makes available to students online.
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 their access to the network or the Internet; upload a worm, virus, "trojan horse," "time bomb" or other harmful form of programming or vandalism; or participate 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; or impersonate another user.
4. Unauthorized commercial transactions. Except when conducting school-related activities (i.e. updating lunch cards, purchasing items from Spirit Shop or Leaning Eagle, etc.), you should not give others private information about you or others, including credit card numbers and social security numbers. Unless authorized by faculty for a class activity or other educational purpose, students and others may not use the computer network or devices for online gaming or gambling. If you have any questions regarding what constitutes an unauthorized commercial transaction under the Policy, please contact the Director of Academics and/or the appropriate Division Administrator (principal, assistant principal).
5. Uses which violate school fraternization policies or uses which promote undue familiarity between those in a faculty/student or superior/subordinate relationship. For example, students who are currently taking classes with faculty becoming online "friends" with such faculty on a social networking site.
6. Use of any personal devices on campus or while attending or participating in a school-sponsored activity or event which violates any policy (for example, sexting using a personal cell phone).
7. Social Media. Student use of social media during school hours, school-sponsored activities, or while using school computer networks, the Internet, or devices must be authorized by a teacher for an approved educational purpose. Any social media activity of a student while using school computer networks, Internet, or devices or while engaging in a school-sponsored activity are subject to the Policy. Any social media activity that is directed at the CHCA community (including administration, teachers, and students) and violates this CHCA Policy shall result in discipline.
8. Sexting. In keeping with the school's responsibility to provide a safe learning environment for all

students, the CHCA Board of Trustees has established the following policy regarding the issue of "sexting." Sexting is the act of sending sexually explicit or suggestive messages, photos, audio, or images via a cell phone, computer, or other digital device. Students engaged in such activities are subject to state laws and school discipline. The school considers sending, sharing, or possessing photos, messages, audio, images, or e-mails that contain sexually explicit or suggestive content, during school hours or in association with any school activity, or at any time where the subject matter involves any student or employee of the school, to be a violation of this policy. Any such violation may result in school discipline, up to and including expulsion and/or the notification of local law enforcement. Students are required to immediately report any such activities to a teacher or a school administrator. Students who report such activity and who are determined to have had no other role in the incident will not be subject to punishment.

9. Making an unauthorized recording or sharing publicly any recording of a class or portion of a class, whether in-person or virtual.

B. **Netiquette.** All users must abide by rules of network etiquette, which include:

1. Remember the "Golden Rule". Be polite and treat others the way you would like to be treated. Do not send abusive messages to others. Hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited.
2. Use appropriate language. Swearing, vulgarities, suggestive, obscene, belligerent, or threatening language are prohibited.
3. Avoid language and uses which may be offensive to other users. Don't use access to make, distribute, or redistribute jokes, stories, or other material, which is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, or religion.
4. Don't assume that the sender of a message gives you their permission to forward or redistribute the message to third parties or to give their information to third parties. This should only be done with permission or when you know that the individual would not object.
5. Be considerate when sending attachments (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.
6. Sending or forwarding "chain letters" is a misuse of the system and may result in the loss of the user's account.
7. Curricular use will take precedence over independent use.

V. INTERNET SAFETY

- A. **General Warning; Individual Responsibility of Parents and Users.** In compliance with applicable federal and state laws and for our students' protection, Internet access at CHCA is filtered. However, even using network filters, all users and their parents/guardians are advised that access to CHCA's network may include the potential for access to materials inappropriate for school-aged pupils. All users must take responsibility for their use of CHCA's computer network and Internet and stay away from these sites. Parents of minors are the best guides in deciding what materials to avoid. Any student that finds that other users are visiting offensive or harmful sites should report such use to the

person designated by CHCA.

- B. Personal Safety.** Be safe. In using CHCA's computer network and the Internet, do not reveal personal information such as your full name, date of birth, home address or telephone number. Do not use your real last name or any other information that might allow a person to locate you without first obtaining the 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 CHCA'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, without the student's permission. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers or Social Security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.
- E. Active Restriction Measures.** CHCA, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering technologies designed to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. CHCA will also monitor students' online activities, through direct observation and/or technological means, to help prevent users from accessing such depictions or any other material that is inappropriate for minors.

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 when appropriate.

VI. SCHOOL PROVIDED DEVICES

When using CHCA-provided technology devices, students must responsibly use the devices. Use of school provided devices is a privilege which may be revoked at any time. Violation of these policies will be subject to normal disciplinary action.

- A. Content and Software** – School equipment is to be used for educational purposes. Music, videos, games and software must be school approved and installed.
- B. Configuration** – Students may not alter the configuration of the device or install passwords on screensavers, BIOS settings menus, or deletion of files or folders. Deletion of some files may also result in a computer failure and may interfere in the ability to complete classwork, directly impacting grades.

- C. **Equipment Repairs** – If the computer fails while in use, CHCA will investigate and determine whether the failure was due to the equipment, or due to improper use. If the failure is due to improper use, the student or parent may be held liable for the cost of repairs and/or replacement.
- D. **Loss or Damage** – If equipment is issued to the student, and the property is damaged, lost or stolen, the student or parent is responsible for the cost or repair or replacement based upon the fair market value at the date of loss. Loss or theft of property must be reported to CHCA within one business day, and a police report must be filed within 48 hours of the occurrence if applicable.
 - a. **If the equipment is stolen:**
 - i. File a police report within 48 hours of the occurrence
 - ii. Notify the Principal immediately, or no later than one business day after the theft
 - b. **If the equipment is lost:**
 - i. The student or parent will be responsible to pay CHCA the total costs associated with replacing the equipment.
 - c. **Students or parents will be charged for the equipment’s replacement or repair if the equipment was deliberately damaged or vandalized.**

VII. PERSONAL DEVICES

If personal electronic devices are used on CHCA’s network or on school property or at a school event or during a school-sponsored activity (even when the student or staff member is using his or her personal data network), use of the personal device must be consistent with the Policy. Internet access on CHCA’s network is recorded, and misuse of personal devices, on or off CHCA’s network while on school property, will be subject to normal disciplinary action.

“Personal device” includes computers, laptops, tablets (e.g., iPads and similar devices), electronic readers/“e-readers” (e.g., Kindles and similar devices); cell phones (e.g. mobile/cellular telephones); smartphones (e.g., iPhone, Android devices, Windows Mobile devices, etc.), and/or other Web-enabled or cellular network-enabled devices of any type.

- A. **Personal Device Use.** Personal devices on campus will be set to “silent” or powered off during class unless they are being used for educational purposes as defined by the instructor. Texting, messaging, surfing the Internet, gaming, and other activity during instructional time, whether in person or virtual, is prohibited unless permitted by a teacher as part of an instructional activity. Personal devices not in use for instruction must be stored out of sight during the school day. During non-class instructional time, the regulations of the family/student handbook define how personal devices may be used, so long as they are not disruptive and such uses comply with this Policy. Any misuse will be subject to normal disciplinary action. Use of personal devices on CHCA’s campus or network, or on a personal data network while on school property or at a school event or during a school-sponsored activity, must comply with this Policy; misuse will be subject to disciplinary action.
- B. **Personal Devices and Student Privacy.** Personal devices, including but not limited to devices with cameras, may not be activated or utilized at any time in any school situation where students have a reasonable expectation of personal privacy. These locations and circumstances include but are not limited to classrooms (whether in person or virtual), gymnasiums (when not in use for events open to the public), locker rooms, shower facilities, rest/bathrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes, whether at CHCA or at another school where a school activity or athletic event is

occurring. The school administration has the authority to make determinations as to other specific locations and situations where use of a personal device is absolutely prohibited. Nothing in this section prevents CHCA from authorizing the recording of classes and/or instructional activities, whether in person or virtual, for the purpose of making the recordings available to students through CHCA's computer network or internet.

- C. Personal Devices during Extra-Curricular Activities.** Students participating in extra-curricular activities and athletics must contact their coach, advisor, or sponsor for his/her rules involving the use of personal devices after school hours or on after-school bus trips. Coaches and advisors will set their rules and enforce consequences involving the use and/or misuse of these devices.
- D. Loss and Damage to Personal Devices.** CHCA assumes no responsibility for theft, loss, or damage to, or misuse or unauthorized use of, personal devices brought onto its property. Students and parents are strongly encouraged to take appropriate precautions, if students possess personal devices at school, to ensure the devices are not left unattended or unsecured.
- E. No Expectation of Privacy.** CHCA reserves the right to monitor, inspect, copy, review and store information contained on students' personal devices while these personal devices are used on school property or at a school event or as part of a school-sponsored activity. Students recognize that they have no expectation of privacy in their own personal devices while on school property or while on the school network.

VIII. PRIVACY

Network and Internet access is provided as a tool for your education. **CHCA 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 CHCA's property and no user shall have any expectation of privacy regarding such materials or devices.

Specifically, students shall have no expectation of privacy in any email, instant message, documents, text message, chat app message, or other electronic communication sent, received, or stored by or through CHCA's computers, computer network, electronic messaging systems, software for learning and productivity, or other devices. Students must not consider these communications to be private or confidential. All student emails, instant messages, documents, text messages, and other information that is accessed, stored, created, received, or sent by or through any of CHCA's computers, computer network, electronic messaging systems, software for learning and productivity, and other devices that are CHCA's property. Authorized CHCA personnel may view student files, communications, data, or any other electronic communication at any time for any reason.

IX. FAILURE TO FOLLOW POLICY

Use of CHCA's computer network and Internet is a privilege, not a right. Any user who violates this Policy, shall be subject to school discipline as determined by the CHCA administration and may have their access to CHCA's computer network and Internet restricted, suspended, or terminated. A user violates this Policy by their own actions and may in certain circumstances violate the Policy by failing to report violations by other users that come to their attention. Further, a user violates this Policy if they permit another to use their account or password to access CHCA's computer network and Internet, including any user whose access has been denied or terminated. CHCA may also take other disciplinary action in such circumstances.

Any violations of this Policy may also result in other behavioral consequences as listed under behavior/conduct guidelines published in CHCA's Family Handbook. Disciplinary action may be determined in keeping with existing procedures and practices regarding inappropriate language or

behavior. When and where applicable, law enforcement agencies may be involved. Violations could result in expulsion.

X. WARRANTIES/INDEMNIFICATION

CHCA makes no warranties of any kind, either express or implied, in connection with providing access to and use of its computer networks and the Internet. 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 their parent(s) or guardian(s) arising out of use of its computer networks or the Internet under this Policy. By signing this Policy, users take full responsibility for their use, and the user who is 18 or older or, in the case of a user under 18, the parent(s) or guardian(s) agree to indemnify and hold harmless CHCA, the Data Acquisition Site that provides the computer and Internet access opportunity to CHCA and all of CHCA's administrators, teachers, and staff from any and all loss, costs, claims or damages resulting from the user's access to CHCA's 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 CHCA if CHCA initiates an investigation of a user's use or access to its computer network and the Internet, whether that use is on a CHCA computer or on another computer outside CHCA's network.

XI. 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, for example, to reflect developments in the law or technology. Such information must be provided by users (or their parents or guardian) if they wish CHCA Registrar to receive such information.

XII. EDUCATION, SUPERVISION AND MONITORING

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Academics, Information Technology services, or designated representatives.

CHCA's Director of Academics, program media specialists, classroom teachers, or designated representatives will provide age-appropriate training for students who use CHCA's Internet facilities. The training provided will be designed to promote CHCA's commitment to:

- The standards and acceptable use of Internet services as set forth in this Policy.
- Student safety regarding: (1) safety on the Internet; (2) appropriate behavior while on online, on social networking Web sites, and in chat rooms; and (3) cyberbullying awareness and response.
- Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").