CTK
CHRIST THE KING
CATHOLIC CHURCH
3001 Belmont Boulevard
Nashville, Tennessee 37212
615-292-2884

Christ the King Church and School
Acceptable Use Policy

Christ the King
School

Executive Summary

- Christ the King's technology resources should be used to advance its mission.
- Using Christ the King's technology resources is a privilege, not a right.
- If this Policy conflicts with federal, state, canon, or diocesan laws, they supersede it.
- Christ the King students are students 24-hours a day and must act consistent with this Policy both on and off campus.
- Any data created on Christ the King's technology systems remains its property.
- Christ the King's technology should be used consistent with the "Golden Rule."
- Users should not represent to third-parties that they speak for Christ the King without the written permission of the Pastor or Principal.
- Users must use Christ the King's technology resources to protect the security of the system and the privacy of others.
- Users who violate this Policy may be subject to disciplinary action.

1.0 Overview

The information technology resources of Christ the King are provided to advance the mission of Christ the King Church and School (collectively "Christ the King"). The intention behind the publication of the Acceptable Use Policy (the "Policy") is not to impose restrictions contrary to Christ the King's culture of openness, trust, and responsibility. Rather, it is to protect Christ the King from illegal or damaging actions by individuals, committed either knowingly or unknowingly.

Using church and school facilities for Internet access by the Christ the King community ("Users", which unless otherwise noted includes priests, deacons, religious, faculty, staff, students (including PREP students), volunteers, parishioners, visitors, contractors, consultants, temporaries, and other workers at Christ the King) is a privilege, not a right. At any time and for any reason, Christ the King may revoke the privilege to use all or any portion of its network and website.

The technology systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP or file sharing programs, are the property of Christ the King, and are to be used to support the mission of Christ the King. Maintaining safe, reliable, and secure systems is a collaborative effort involving the participation and support of its Users. It is the responsibility of Users to know and adhere to the Policy. Please contact the Systems Administrator, Don Boehm, don.boehm@ctk.org, for any explanations or clarifications needed.

2.0 Purpose

The purpose of the Policy is to outline the acceptable use of technology systems at Christ the King. The Policy is in place to protect both Users and Christ the King. Inappropriate use exposes Christ the King to threats including, but not limited to, virus attacks, compromise of network systems and services, legal issues, and reputational and integrity risks. If this Policy conflicts with any law, including canon law or the rules and policies of the Diocese of Nashville, including, but not limited to, the Guidelines for Use of Social Media established by the Diocese, then the latter supersedes this Policy.

3.0 Scope

This Policy has specific provisions for students at Christ the King School, and provisions that apply to students likewise apply to minors who participate in ministries for children and young adults. A student at Christ the King is a student 24 hours a day and is expected to act consistently with his or her enrollment in a Catholic school, which includes abiding by its rules and regulations both on and off campus. For clarifications on how the Policy applies to minors, the School Principal is the primary point of contact. For clarifications on how this Policy applies to minors who participate in ministries sponsored by Christ the King Church, the Director of Child and Youth Ministries is the primary point of contact. This Policy applies to all equipment and system software or software services owned, leased, or otherwise sponsored or used by Christ the King and equipment, software systems, or software services owned, leased, or otherwise sponsored or used by other parties used on the Christ the King network.

4.0 Policy

4.1 General Use and Ownership

1. While Christ the King's network administration desires to provide a reasonable level of privacy, Users should be aware that all data created on its systems is the property of Christ the King. Because of the need to protect the network, administrators cannot guarantee the confidentiality of information stored on any network device belonging to Christ the King.
2. Community members, students, faculty and staff are responsible for exercising good judgment regarding the reasonableness of personal use. Commercial uses are prohibited. If there is any uncertainty, Users should consult the Systems Administrator identified above or the School Principal.
3. For security and network maintenance purposes, administrators at Christ the King may at any time monitor and search any equipment, systems, network traffic, and any media brought onto Christ the King's campus or cloud-based storage accessed from a computer on campus.
4. Christ the King reserves the right to audit networks and systems on a periodic basis to ensure compliance with the Policy.
5. Christ the King relies upon the active cooperation of Users and the responsibility and integrity of students to maintain safe and secure facilities for approved uses of the technology in the School. Anyone using the computing facilities must adhere to that same standard.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized Users are responsible for the security of their passwords and accounts.
2. All PCs, laptops, workstations and other Internet-connected devices should be secured by logging-off when the system will be unattended.
3. Postings by Users from a Christ the King email address to newsgroups, weblogs, mailing lists, or other discussion or bulletin boards should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Christ the King Church and School, unless posting is in the course of normal school or parish duties.
4. All systems connected to the network, whether owned by the User, Christ the King, or a third-party, shall have approved, continually executing virus-scanning software with a current virus signature database. Users must notify immediately the Systems Administrator of any viruses detected by the software or of any activity that appears to be virus-related.
5. Users must use extreme caution when opening e-mail attachments received from unknown senders that may contain viruses, e-mail bombs, or Trojan horse code. Likewise, Users should not use any external storage devices on any Christ the King device unless they are familiar with the contents and its safety and they have obtained permission from the Pastor, Principal, or School faculty.
6. Users should be aware that Christ the King cannot guarantee security and privacy in all cases, especially for personal or unlawful use of information technology resources. Christ the King's System Administrator(s) will use reasonable efforts and legal practices to secure resources and maintain privacy.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a system if that system is disrupting production services).

Under no circumstances are Users at Christ the King authorized to engage in activity that is illegal under local, state, federal or international law or contrary to canon law or the rules and policies of the Diocese of Nashville while utilizing Christ the King resources. The lists below are not exhaustive, but are an attempt to provide a framework for activities that fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

System and Network Activities

1. Defeating or attempting to defeat content filtering systems.
2. Revealing an account password to others, allowing use of an account by others, or using the accounts of others.
3. Circumventing user authentication or security of any host, system, network or account, or disguising or attempting to disguise the identity of a host, system, account, or service on the network.
4. Using or attempting to use administrative accounts or other network accounts without authorization.
5. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property or similar laws or regulations, including, but not limited to, using classified government information and the installation or distribution of "pirated" or other software products not appropriately licensed for use by Christ the King.
6. Unauthorized duplication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, copyrighted video, and the installation of any copyrighted software for which Christ the King or the User has no valid, active license is strictly prohibited. Fair use of copyrighted materials is possible; consult the Systems Administrator or the librarian for assistance in determining fair use.
7. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal and prohibited.
8. Intentionally, recklessly, knowingly, or negligently introducing viruses, Trojans, worms, or other commands, scripts, or programs intended to damage or degrade computer systems or network resources or to make unauthorized access of networks or systems.
9. Using Christ the King systems to actively engage in procuring, viewing, and/or transmitting material in violation of sexual harassment or hostile workplace laws, canon law, Diocesan rules and policies, or the teachings of the Catholic Church. This includes morally objectionable materials, files, images, text, or other content.
10. Making fraudulent offers of products, items, or services originating from any Christ the King account or conducting advertising, marketing, sales, or distribution activities for commercial products, items, or services unrelated to the mission of Christ the King.
11. Effecting security breaches or disruptions of network communication of either Christ the King’s network or other external networks. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless it is within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Port scanning, intrusion detection, or other security scanning is prohibited by anyone other than the Systems Administrator(s) charged with responsibility for system security.
13. Executing any form of network monitoring that will intercept data not intended for the User’s system, unless this activity is a part of the User’s normal job/duty.
14. Interfering with or denying service to any other user (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, intending to interfere with, or disable, a user's terminal session, by any means, locally or via the network.

16. Providing information about, or lists of, Christ the King faculty, staff, students, or parishioners to anyone outside the Christ the King community. This must be approved in advance in writing by the Systems Administrator, Principal, or Pastor.
17. Use of wireless access to network resources by students without the prior written permission of the technology administrators, Principal, or Pastor.
18. Use of resources that is wasteful or monopolizes system resources at the expense of other Users.
19. Use of peer-to-peer file sharing software to access, share, or trade any files.

Email and Communications Activities

1. Any form of harassment, insult, intimidation, embarrassment, or obscenity via email, text messaging, telephone or paging, or any other social media or electronic communications device or platform, whether through language, frequency, or size of messages.
2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals or businesses (email spam).
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Christ the King's networks or from other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Christ the King or connected via Christ the King's network.
7. Posting the same or similar messages to large numbers of Usenet newsgroups (newsgroup spam).
8. Political lobbying of any nature. Use of Christ the King facilities to lobby for political candidates jeopardizes Christ the King’s tax-exempt status and violates the terms under which some donations and grants are made to Christ the King.

Prohibited activities specific to students

1. Plagiarism. Student use must follow the Academic Dishonesty Policy at http://cksraiders.org/parents.htm#policies.
2. Vandalism, including unapproved editing, copying, interference with, or destruction of others’ work, unauthorized software installation or modification, and introduction of computer viruses, Trojan horse, keystroke logging, or other computer malware.
3. Password theft or sharing.
4. Transmission of any personal information such as last name, home address, email address, or telephone number from a school computer, either one’s own or another student’s, or falsification of such personal information.
5. Use of email, text messaging, or instant messaging software, whether using personal computers, cell phones, smart phones, or other Internet- or telephone network-connected devices, and any social media account or platform, on Christ the King’s property from 7:00 a.m. to 6:00 p.m., Monday through Friday, without explicit permission of a teacher or the Principal.
6. Use or transmission of harassing, insulting, threatening, embarrassing, or obscene materials.
7. Use or transmission of materials that violate the standards of conduct or other policies published in the Student Handbook.
8. Installation of software on Christ the King systems or installation of Christ the King software on other systems, whether standard commercial software, shareware, or freeware, or downloading commercial software, shareware, or freeware software from external or Internet sources.
9. Use of school name or logo on any external site, webpage, email list, message board, social networking site or system, without the prior written authorization from the Principal.
10. Use of school wireless network requires permission of the System Administrator or Principal.

4.4 Email Retention Christ the King provides email to employees for the purpose of general communications. No special measures are taken to retain or archive email messages due to issues of cost and complexity. All official communications or documentation should be conducted in print and archived in correspondence files. Please treat email as the equivalent of a postcard or phone conversation and use postal mail for official communications or documentary notifications. Please contact the Systems Administrator for any needed clarifications.

4.5 Blogging, Social Networking, Photo, Audio, and Video Publishing

1. This Policy includes, but is not limited to, personal blogs and personal websites, and services such as, but not limited to, Facebook, MySpace, LinkedIn, Twitter, Digg, Plaxo, and Bebo, among other similar means of publishing information or intellectual property, photos, audio clips, or videos.
2. Blogging or social networking by Users, whether using Christ the King's property and systems or personal computer systems, is also subject to the terms and restrictions in the Policy. Limited and occasional use of Christ the King 's systems to engage in blogging or social networking is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate this Acceptable Use Policy, is not detrimental to Christ the King's best interests, and does not interfere with an employee's regular work duties. Blogging or social networking from Christ the King's systems is also subject to monitoring. Users are prohibited from revealing any confidential or proprietary information when engaged in blogging or social networking.
3. Users shall not engage in any blogging or social networking activities that may harm or tarnish the image, reputation, and/or goodwill of Christ the King and/or any of its community members. Users are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging.
4. Users may also not attribute personal statements, opinions, or beliefs to Christ the King when engaged in blogging or social networking activities. If a User is expressing beliefs and/or opinions in blogs or social networking sites, the User may not, expressly or implicitly, represent themselves as an employee or representative of Christ the King. Users assume all risk associated with blogging and social networking.
5. Users are encouraged to use the following guidelines in using blogging or social networking media or services:
    - Do not be anonymous.
    - Be relevant to your area of expertise, and be careful not to overstep the boundaries of your area. Don't use expertise in one area to claim authority outside of that area.
    - Always be professional, courteous, honest, and respectful.
    - Use the "good judgment" test – if you were to look back at your contribution from a perspective a year in the future, would you be happy with your posting or contribution – does it show that you exercised good judgment?
6. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export of controlled materials, Christ the King's trademarks, logos, and any other Christ the King intellectual property may not be used in connection with any blogging or social networking activity. Users are requested to report unofficial sites that use the diocesan, parish, or school logo or name without permission.
7. Users may find valid and important professional and personal uses for blogging and social networking sites. School personnel, specifically teachers, staff, and adult volunteers, are prohibited from networking or making specific connections with students through social networking sites. Those with a legitimate need to use Internet-based media for communicating with students or other minors are referred to the Principal and the Director of Child and Youth Ministries for approved means and methods.
8. Students are prohibited from using blogging or social networking websites from Christ the King's campus except under the direct supervision of teachers or staff. Students may not use their own personal communications devices (smartphones, tablets, PCs, or other Internet-connected devices) to access social networking websites from the Christ the King campus. For all other Users, the Principal's judgment is the determinant as to whether a given website falls under the description of "social networking." Posting of messages to personal pages or "walls" and the use of and using social networking instant messaging are prohibited from any communications devices, whether cellphones, smartphones, PCs, or other Internet- or telephone network-connected devices.

9. Students are prohibited from posting photos, audio clips, or videos to blogs or social networking sites or to other publishing sites from the Christ the King campus, using campus-owned computers, or personal equipment, including, but not restricted to, computers, smartphones, cellphones, or other Internet- or telephone network-connected devices, except under the direct supervision of teachers or staff.

5.0 Enforcement

Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment. Any student found to have violated this Policy may be subject to disciplinary action, including termination of computer rights, failure of computer class, suspension, and expulsion from school. Any parishioner found to have violated this Policy may have his or her use of Christ the King's facilities revoked. In addition to the above discipline, appropriate legal action may be taken. Christ the King will cooperate with law enforcement authorities in prosecuting criminal action when appropriate. Monetary charges may be sought for damage necessitating legal expense, repair or replacement of equipment or software, as well as any related costs for time and materials required to make systems operational.

6.0 Revision History

v. 1.0 Original policy.

v. 2.0 First draft, March 7, 2003, adapted from SANS sample policies, http://www.sans.org/resources/policies/.

v. 2.1 Revisions incorporating materials from original policy, April 3, 2003.

v. 2.2 Incorporated recommendations from D. Lovell, add reference to external definition of plagiarism.

v. 2.3 Added file sharing prohibition, July 29, 2003.

v. 2.4 Revisions from Christine Caron-Gebhardt, August 5, 2003. Changes also made to Upper and Lower Grade documents.

v. 3.0 Added explicit IM prohibition for students, prohibition on defeating content filters, June 25, 2004. Reviewed with no changes made, August 3, 2005.

v.4.0 Added prohibition on use of school name, logo by students without permission, August 3, 2006.

v.5.0 Added email retention policy, section 4.4, August 9, 2007.

v.6.0 Further specifications to scope in section 3. Added explicit prohibition of text messaging, restrictions on blogging, use of social networking, publishing videos, audio clips and photos. Materials adapted from Rick Vanover's Tech Republic sample social networking policy and from SANS sample policies on blogging and social networking in section 4.5, August 6, 2009.

v. 7.0 Added requirement that students have permission of Principal to use campus wireless network in 4.3; minor edits to 4.5.

v. 8.0 Revisions from School Board, January 19, 2016. School Board voted to use one AUP and to cease using Upper and Lower Grade documents.

Last reviewed July 12. 2017