



Christ the King Church and School Acceptable Use Policy

Age-appropriate versions are available for students.
Contact Don Boehm, ext. 303.



1.0 Overview

The information technology resources of Christ the King are provided to advance the missions of Christ the King Church and School. The intention behind the publication of an Acceptable Use Policy is not to impose restrictions that are contrary to Christ the King's culture of openness, trust and responsibility. Rather, we are committed to protecting the Christ the King community from illegal or damaging actions by individuals, committed either knowingly or unknowingly.

Our technology systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Christ the King, and are to be used in support of the mission of our Church and School. Maintaining safe, reliable, and secure systems is a collaborative effort involving the participation and support of every member of the Christ the King community who uses our information systems. It is the responsibility of every computer user to know these guidelines, and to conform his or her activities accordingly. Please contact the systems administrator, Don Boehm, don.boehm@ctk.org or 615-292-2884, ext. 303, for grade-level appropriate versions of this document or for any explanations or clarifications needed.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Christ the King. These rules are in place to protect both the members of the community and the parish and school. Inappropriate use exposes Christ the King to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to parishioners, students, employees, contractors, consultants, temporaries, and other workers at Christ the King, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Christ the King and equipment owned or leased by other parties which is 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 the data they create on the parish systems remains the property of Christ the King. Because of the need to protect our network, management cannot guarantee the confidentiality of information stored on any network device belonging to Christ the King Church and School.
2. Community members, students 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 administrator responsible for technology management, the School Principal, or the Pastor.
3. For security and network maintenance purposes, administrators at Christ the King may monitor equipment, systems and network traffic at any time.
4. We reserve the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
5. We rely upon the active cooperation of parents and the responsibility and integrity of students to maintain safe and secure facilities for approved uses of our technology in our school. Parishioners, staff, and anyone who uses our computing facilities are asked to live up 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 and workstations should be secured by logging-off (control-alt-delete for Win2K users) when the system will be unattended.
3. Postings by employees 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 used by the employee that are connected to the network, whether owned by the employee or Christ the King Church or School, shall be continually executing approved virus-scanning software with a current virus signature database. Notify the systems administrator of any viruses detected by the software or of any activity which appears to be virus-related.
5. Employees must use extreme caution when opening e-mail attachments received from unknown senders which may contain viruses, e-mail bombs, or Trojan horse code.
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 system administrators will use best efforts and best practices to secure resources and maintain privacy, particularly for records protected by statute.

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 have a 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 any 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-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

System and Network Activities

1. 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, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Christ the King Church and School, or use of classified government information.
2. Unauthorized copying 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 Church or School or the end user does not have a 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.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal and prohibited.
4. 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.
5. Using or attempting to use administrative accounts or other network accounts without authorization.
6. Defeating or attempting to defeat content filtering systems.
7. Revealing your account password to others or allowing use of your account by others.
8. Using Christ the King systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws, canon law, or Diocesan rules and policies. This includes morally objectionable materials, files, images, text or other content.

9. Making fraudulent offers of products, items, or services originating from any Christ the King account; conducting advertising, marketing, sales or distribution activities for commercial products, items, or services unrelated to the mission of our Church and School.
10. Effecting security breaches or disruptions of network communication of either the Christ the King network or other external networks. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are 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.
11. Port scanning, intrusion detection or other security scanning is expressly prohibited by anyone other than systems administrators charged with responsibility for system security.
12. Executing any form of network monitoring which will intercept data not intended for the employee's system, unless this activity is a part of the employee's normal job/duty.
13. 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.
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, with the intent 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 staff, students, or parishioners to parties outside the Christ the King community.
17. Use of wireless access to network resources without prior written permission of the technology administrators, principal or pastor.
18. Use of resources which is wasteful or which 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, telephone or paging, whether through language, frequency, or size of messages.
2. Knowingly or negligently introducing viruses, trojans, worms, or other commands, scripts or programs intended to damage or degrade other computer systems or networks or to make unauthorized access of other networks or systems.
3. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam.)
4. Unauthorized use, or forging, of email header information.
5. 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.
6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
7. 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.
8. Posting the same or similar messages to large numbers of Usenet newsgroups (newsgroup spam).
9. Political lobbying. Use of Christ the King facilities to lobby for political candidates or causes jeopardizes our tax-exempt status and violates the terms under which some donations and grants are made to our school.

Prohibited activities specific to students

1. Plagiarism. We use the definition from *Hodges' Harbrace Handbook*, Hodges et al, 14th edition, sect. 38d, pp. 574-578.
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 students, or falsification of such personal information.
5. Use of email or instant messaging software 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 which 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 prior written authorization from Principal.

4.4 Email Retention Christ the King Church and School 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 appropriate 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 church or school administration for any needed clarifications.

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 for computer class, and expulsion from school. Any parishioner found to have violated this policy may have rights to use Christ the King facilities revoked. Christ the King will cooperate with law enforcement authorities in prosecuting criminal action when appropriate.

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 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.