Network Security Policy and Usage

OVERVIEW

Internet access to global electronic information resources on the World Wide Web is provided to clergy, religious, employees, volunteers and students to provide ease in obtaining data and technology to assist in their respective ministries, duties or studies.

Our technology systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol (FTP), are the property of the diocese/parish/school, and are to be used in support of the mission of the Catholic Church. Maintaining a safe, reliable, and secure system is a collaborative effort involving the participation and support of every individual who uses our information systems. It is the responsibility of every computer user to know and conform to these guidelines.

PURPOSE

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

SCOPE

This policy applies to anyone using the diocese/parish/school technology system, including parishioners, students, employees, contractors, consultants, temporaries, volunteers, and other workers, as well as all personnel affiliated with third parties. This policy has specific provisions for students. The provisions which apply to students, likewise apply to minors who take part in ministries for children and young adults. For clarifications on how this policy applies to minors, the school principal, pastor, or the religious education director is the primary point of contact.

GENERAL USE AND OWNERSHIP

While the network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on parish systems remains the property of the diocese/parish/school. Because of the need to protect our network, management cannot guarantee the confidentiality of information stored on any network device and no rights of privacy exist.

All users are responsible for exercising good judgment regarding the reasonableness of personal use. Commercial use is prohibited. If there is any uncertainty, users should consult the administrator responsible for technology management, the School Principal, or the Pastor.

The equipment, services and technology provided to access the web are the property of the diocese/parish/school. For security and network maintenance purposes, administrators may monitor equipment, systems and network traffic at any time. We reserve the right to audit networks and systems, monitor internet traffic, retrieve and read any data composed, sent, or received on a periodic basis to ensure compliance with this policy.

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. All users of our computer facilities are asked to live up to that same standard.

UNACCEPTABLE USE
The Diocese/Parish has taken the necessary actions to assure the safety and security of our network. Any individual who attempts to disable, defeat or circumvent security measures is subject to disciplinary action up to and including dismissal. The following are examples of actions and activities that are prohibited:

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 the diocese/parish/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 the diocese/parish/school or the end user does not have a valid, active license is strictly prohibited.
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, disable, 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. Stealing, using or disclosing another user’s password or code without authorization.
8. Using any network 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. Security breaches or disruptions of network communication. 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.
10. Port scanning, intrusion detection or other security scanning is expressly prohibited by anyone other than systems administrators charged with responsibility for system security.
11. 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.
12. 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.
13. Interfering with or denying service to any other user (for example, denial of service attack.)
14. 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.
15. Providing information about, or lists of, staff, students, or parishioners to parties outside the diocese/parish/school.
16. Use of wireless access to network resources without prior written permission of the technology administrators, principal or pastor.
17. Use of resources which are wasteful or which monopolize system resources at the expense of other users.

18. Use of peer-to-peer file sharing software to access, share or trade any files.
19. Using internet for participation in Chat rooms or other web-based forums unrelated to ministry, duties or studies.
20. Engaging in any other illegal activities.

DISCRETION

Those who minister and work in pastoral settings must take great care to be consistent in representing the worth of their character online. Clear communication and respect for boundaries is needed at any level of contact. Emails, text messages, blog postings or comments, and YouTube videos are all public forums from which a permanent record can be obtained. As a representative of the Church, users should be diligent in avoiding situations which might be the source of scandal for themselves or others. Furthermore, those to whom we minister must be educated on the public nature of such communication. Confidential information should never be sent via email.

EMAIL, INSTANT MESSAGING, AND VIDEO CHATTING

Email and instant messaging (IM) allows for increased flexibility and immediacy in communication. When appropriately combined with face-to-face communication, email and IM can significantly enhance how we minister to others. The same boundary issues that must be respected in oral communication must be respected in written ones. Good judgment should always be used with text based communication tools. Parental/guardian consent needs to be obtained when communicating by email or instant messaging with young people.

- Maintain a separate email account for your professional communication and only use this account when communicating with youth.
- Email, IM, and Video Chatting communication should only be used with matters that deal with an individual’s professional relationship. Communicate only about matters that address the business-at-hand of your ministry.
- Care should be taken to maintain professionalism and appropriate boundaries in all communication.
- There should be absolutely no personal exchanges.
- Electronic communication can be easily misinterpreted. Communicate in person whenever possible. Before sending an email, ask yourself if someone might “read something into it” that you didn’t intend. If you think your email might somehow be misunderstood, don’t send it.
- If there is any potential for embarrassment or harm, reconsider sending the email or IM.
- Be cautious when sending an email, especially either in haste and/or when emotions are involved.

Always avoid any communication that might be construed as having inappropriate sexual or romantic overtones. Do not reply to any such email from a minor. Instead, make a copy of such inappropriate communication and notify your supervisor. Remember, there is no such thing as a private email. All emails and IM’s can be logged, archived, and forwarded to other parties. Your communication can quickly become a public matter.

- Unlike verbal communication, any form of written communication has a form of permanence.
- There should be no expectation of privacy.
- At no time is one-on-one video chatting appropriate with young people.

MINISTRY WEB PAGES

Anyone who establishes a ministry web presence should make a commitment to this vehicle of communication. Web pages, especially the index or main page(s), should be regularly updated. As with any ministry effort, there should be an intentional plan and set of goals regarding establishing and maintaining a web presence. Great care should be used to protect people on a web page that is publicly accessible.

- Personal information should never be made available (i.e. home address, home or cell number, home email address, etc.).
- Written authorization must be obtained from parent/guardian before posting photos or videos of young people.
- Pictures or videos should not be captioned with a young person's name unless the parent/guardian has given you written authorization to do so.
- Never use a picture or video that might be considered embarrassing or unflattering.
- Care should be taken to protect the reputation of our church membership. If individuals are uncomfortable with a particular photo or video, it should be immediately removed from the website.

SOCIAL NETWORKING

A social network service utilizes software to build online social networks for communities of people who share interests and activities. Most services are primarily web-based and provide various ways for users to interact, such as chat, messaging, email, video or voice chat, file sharing, blogging, discussion groups, etc.

Social networking has become a part of everyday life, as a variety of social networking tools are being used by millions of people on a regular basis. The most popular sites include www.facebook.com, www.myspace.com, and www.twitter.com. Social networking has revolutionized the way we communicate and share information with one another. Therefore, it can be a way to connect people with the church and the church's activities with people.

On any social network site, personal opinions and discussions are often conducted. It is essential for users to remember that even on the World Wide Web, others may recognize them as representing the values of the Catholic Church.

- If a professional staff minister wants to use social networking sites for ministry purposes, a professional social networking account should be created that is separate from their personal account. This account should be seen as an official extension of the ministry organization's web presence, administrated by an adult, and approved by the pastor or supervisor in which the social networking site will be used. Volunteers should not set up a special ministry site without the permission of the professional staff minister and/or the pastor.
- There is a difference between initiating a 'friend request' and accepting one. Pastoral ministers must not initiate and 'seek' friends on the professional social networking account. Outside individuals must request you as a friend first.
- Using the Internet for accessing information about the people to whom we minister is a violation of their privacy, even if that information is publicly accessible.

SOCIAL NETWORKING WITH MINORS

Anyone who ministers and works in pastoral settings with young people with a "personal" social networking site should never advertise that site nor 'friend' a young person to their "personal" site. If you become aware of information that is in the public domain of such a site, you are responsible for information that must be reported if a minor has been abused or is under threat of harm.

"Best Practices"
Ideally, the professional minister, with permission from the pastor/supervisor, should create an online group on social networking sites that both young people and adults can join and interact without full access to one another's profile.

BLOGGING

One method to develop and disseminate content is through a blog. The word "blog" is short for 'Web log' or 'Web-based log.' Those who minister and work in pastoral settings may only establish and publish through ministry-based blogs with the prior approval of their pastor or supervisor. As a representative of the Church, blogging should be conducted in a professional manner for ministry purposes only. As with any professional communication, ministry blogs should **not** be used:

- For any personal communication or agenda.
- To conduct or promote outside business activities.
- To defame or cause defamation of the character of any individual, organization or institution.
- To divulge any personal information about an individual or jeopardize their safety in any other way.

"Best Practices"
Ministry based blogs can publish information including, but not limited to:

- Fliers for upcoming activities, permission forms, calendar, and ministerial updates
- Additional links and references for faith formation
- Sacramental preparation information including: class times, checklists, sponsor resources, parent resources, etc.
- Descriptions of projects, including procedures, expectations, and suggested parent involvement
- Bible Studies and other spiritual links and prayer resources
- Achievements of parishioners

BLOG DISCIPLINE (needs to support the student handbook)
The question that will come up frequently is "Can students with an "anti-school" message be disciplined?" The following is a recommendation that can be modified based on your student handbook.

- If the student handbook is worded so students are on notice that behavior will subject them to discipline, they can be disciplined.
- The handbook should be worded to apply to out-of-school conduct that violates school rules.
- The handbook should be worded to address behavior regardless of whether it is verbal, physical, written, graphic or electronic.
- Distinguish violation of school rules from anti-school messages.

ONLINE GAMING

Those who minister and work in pastoral settings with young people should take care in their involvement with online gaming. While this may be a recreational alternative, for many it is also an opportunity for social networking. Pastoral ministers should take care of protecting their online game identities so that appropriate boundaries are maintained.

DEFINITIONS

1. **Computer Use** — Shall mean and include the use of school computers and networks and other technology resources including, without limitation, computers and related technology equipment or networks, all forms of email or electronic communication, websites and the Internet including onsite or by dial-up or remote access thereto through school accounts, as well as any use which involves visual depictions, audio, video or text, in any form.

2**. Computer User** — Shall mean and include any parishioners, students, employees, contractors, consultants, temporaries, volunteers, and other individuals who engage in Computer Use as defined herein.
 3. **Access to the Internet** — A computer shall be considered to have access to the Internet if such computer is equipped with a modem or is connected to a computer network which has access to the Internet, or which accesses the Internet by dial-up or remote access using an Internet account.

4. **Minor** — Shall mean an individual who has not attained the age of 18.

5. **Obscene** — Shall have the meaning given such term in Section 1460 of Title 18, United States Code.

6. **Child Pornography** — Shall have the meaning given such term in Section 2256 of Title 18, United States Code.

7. **Hacking** — Shall mean Computer Use or using the Internet to attempt to gain unauthorized access to proprietary computer systems.

8. **Technology Protection Measure —** Shall mean and refer to a proxy server that blocks and/or filters Internet access.

9. **Adult** — Shall mean and refer to individual age 18 or older.

PHOTOGRAPH AND VIDEO CONSENT FORM:

From time to time, pictures and video may be taken of youth ministry events and gatherings. We would like to be able to use these photographs and videos for flyers, parish and diocesan publications, and the ministry website. Written consent of both the student and parent/guardian is required. Names will not be posted unless written authorization is given by the student and parent/guardian, and then only first names will be used. If there are concerns about pictures or videos posted on the website, please contact the ministry coordinator or webmaster, and they will promptly be removed.

I/We, the parent(s)/guardian(s) of this youth (name) ____________________, authorize and give full consent, without limitation or reservation, to (parish/school) __________________, to publish any photograph or video in which the above named student appears while participating in any program associated with (parish/school)__________________ ministry. There will be no compensation for use of any photograph or video at the time of publication or in the future.

Student Signature: ______________________________________ Date: ____________

Parent/Guardian Signature: _______________________________ Date: ____________

Parent/Guardian Signature: _______________________________ Date: ____________