

Acceptable Use Policy

Conception Abbey, Inc.

1.0 Purpose

The computing resources at Conception Abbey support the educational, instructional, research, and administrative activities of Conception Seminary College, the business activities of the Printery House, the administrative, and business activities of the Abbey proper, and the institutional activities of the Development Office. The use of these resources is a privilege that is extended to members of the broader Abbey community. As a user of these services and facilities, you have potential access to valuable resources, to sensitive data, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, Conception Abbey will take remedial or disciplinary action, including the restriction and loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as local, state, and federal laws develop and change.

This document establishes specific requirements for the use of all computing and network resources at Conception Abbey.

2.0 Scope

This policy applies to all users of computing resources owned or managed by Conception Abbey.

Individuals covered by the policy include monks, seminary faculty and visiting faculty, staff, seminarians, alumni, guests, external individuals and organizations accessing network services via Conception Abbey's computing facilities.

Computing resources include all Abbey owned, licensed, or managed hardware and software, and use of the Abbey network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments (such as the Abbey Library and Information Technology Services), personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the Abbey's network services.

2.1 Your Rights and Responsibilities

As a member of the community, the Abbey provides you with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a monk, employee, seminarian, or guest), and of protection from abuse and intrusion by others sharing these

resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the Abbey that apply to appropriate use of the it's technologies and resources. You are responsible for exercising good judgment in the use of the Abbey's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

As a representative of the Conception Abbey and Seminary communities, you are expected to respect the Abbey's good name in your electronic dealings with those outside the institution.

3.0 Policy

3.1 Acceptable Use

- You may use only the computers, computer accounts, and computer files for which you have authorization.
- You may not use another individual's account, or attempt to capture or guess other users' passwords.
- You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to the Abbey for all use of such resources. As an authorized Conception Abbey user of resources, you may not enable unauthorized users to access the network by using an Abbey computer or a personal computer that is connected to the Abbey network.
- The Abbey is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
- You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing the Abbey's network and computing resources.
- You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- You must not develop or use programs that disrupt other computer or network users or that damage software or hardware components of a system.
- Do not download and/or use tools that are normally used to assess security or to attack computer systems or networks (i.e. password "crackers", vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so by I.T. Services.

3.2 Fair Share of Resources

Information Technology Services, and other Abbey and Seminary departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others. The campus network, computer clusters, mail servers and other central computing resources are shared widely and are limited; therefore, resources must be used with consideration for others who also use them.

The Abbey may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

3.3 Adherence with Federal, State, and Local Laws

As a member of the Conception Abbey and Seminary community, you are expected to uphold local ordinances and state and federal laws. Some Abbey guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of the Abbey's computing and network resources you must:

- Abide by all local, state, and federal laws.
- Abide by all applicable copyright laws and licenses. Conception Abbey has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.
- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
- Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless you have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

3.4 Other Inappropriate Activities

You may use the Abbey's computing facilities and services for those activities that are consistent with the business, administrative, educational, research, and public service mission of the Abbey and Seminary.

Other prohibited activities include:

- Activities that would jeopardize the Abbey's tax-exempt status.
- Use of the Abbey's computing services and facilities for political or personal economic gain.

3.5 Privacy & Personal Rights

- All users of the Abbey's network and computing resources are expected to respect the privacy and personal rights of others.
- Do not access or copy another user's email, data, programs, or other files without permission.
- Be professional and respectful when using computing systems to communicate with others; the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to administrative discipline as well as legal action by those who are the recipient of these actions.

While Conception Abbey does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, for the business needs of the Abbey. Access to files on Abbey owned equipment will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the business manager in conjunction with his appointed counsel. External law enforcement agencies and Public Safety may request access to files through subpoenas and other legal processes. All such requests must be approved by the business manager. Information obtained in this manner can be admissible in legal proceedings or in an administrative hearing.

3.51 Privacy in Email

You should not expect email privacy when connected to the Conception Abbey network. Abbey staff may inadvertently be exposed to email in the course of their work. In cases where information is inadvertently exposed, staff are required to keep the contents confidential. Remember that email is easily redistributed and may be read by people beyond the original recipient list.

3.52 Important Notice for Monks, Employees, and Seminarians:

Electronic information systems and network services are made available for use by monks, employees, and seminarians to conduct Abbey business. Subject to applicable laws, the Abbey, through its authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user. Users are advised that electronic data (and communications using the Abbey network for transmission or storage) may be reviewed and/or accessed by authorized Abbey officials for purposes related to Abbey business. The Abbey has the authority to access and inspect the contents of any Abbey equipment, files or email on its systems. If such circumstances arise where files (including email) are not accessible to authorized Abbey officers due to circumstances such as unexpected absence, death, or termination of employment or studies, the business manager will authorize the specific access as necessary.

3.53 Email

- You should not expect email privacy when connected to the Conception Abbey network. I.T. Services staff may inadvertently view email in the course of their work. In cases where information is inadvertently exposed, I.T. Services personnel are required to keep the contents confidential.
- Remember that email is easily redistributed and may be read by people beyond the original recipient list.
- Mailbox size limits have been imposed to conserve on server resources. Individuals and departments need to demonstrate a need for a quota increase before changes to their email account is made.

Because of the potentially harmful nature of the content of many messages or attachments, I.T. Services currently:

- Does not deliver messages containing attachments that have been identified as worms by our current anti-virus vendor;
- Deletes all scripted or executable attachments;
- Blocks messages from external mailers identified by third-party vendors as known spammers
- Scans all incoming, intercampus, and outgoing email.

3.6 User Compliance

When you use any Conception Abbey computing or electronic services, or accept any issued computing accounts, you agree to comply with this and all other computing related policies. You have the responsibility to keep up-to-date on changes in the computing environment, as published, using Abbey electronic and print publication mechanisms, and to adapt to those changes as necessary.

Approved by the IT Services Oversight Board 8-05

Network Connection Policy

1.0 Purpose

This policy is designed to protect the Conception Abbey campus network and the ability of monks, employees, seminarians, and guests of the community to use it. The purpose of this policy is to define the standards for connecting computers, servers or other devices to the Abbey's network. The standards are designed to minimize the potential exposure to Conception Abbey and our community from damages (including financial, loss of work, and loss of data) that could result from computers and servers that are not configured or maintained properly and to ensure that devices on the network are not taking actions that could adversely affect network performance.

Conception Abbey provides a secure network for our educational, research, instructional, business, and administrative needs and services. An unsecured computer on the network allows denial of service attacks, viruses, Trojans, and other compromises to enter the Abbey's campus network, thereby affecting many computers, as well as the network's integrity. Damages from these exploits could include the loss of sensitive and confidential data, interruption of network services and damage to critical internal systems. Institutions that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computers, servers and other devices to the Abbey network must follow specific standards and take specific actions.

2.0 Scope

This policy applies to all members of the larger Conception Abbey community or visitors who have any device connected to the Abbey network, including, but not limited to, desktop computers, laptops, servers, wireless computers, specialized equipment, cameras, environmental control systems, and telephone system components. The policy also applies to anyone who has systems outside the campus network that access the campus network and resources. The policy applies to Abbey-owned computers (including those purchased with grant funds), personally-owned or leased computers that connect to the Abbey network.

3.0 Policy

3.1 Appropriate Connection Methods

You may connect devices to the campus network at appropriate connectivity points including voice/data jacks, through an approved wireless network access point, via a VPN or SSH tunnel, or through remote access mechanisms such as DSL, cable modems, and traditional modems over phone lines.

Modifications or extensions to the network can frequently cause undesired effects, including loss of connectivity. These effects are not always immediate, nor are they always located at the site of modifications. As a result, extending or modifying the Abbey network must be done with the approval of I.T. Services before such modifications are made. Exceptions will be made by I.T. Services for approved personnel in departments who can demonstrate competence with managing the aforementioned hardware.

3.2 Network Registration

Users of the campus network may be required to authenticate when connecting a device to the network. I.T. Services maintains a database of unique machine identification, network address and owners for the purposes of contacting the owner of a computer when it is necessary. For example, I.T. Services would contact the registered owner of a computer when his or her computer has been compromised and is

launching a denial of service attack or if a copyright violation notice has been issued for the IP address used by that person.

3.3 Responsibility for Security

Every computer or other device connected to the network, including a desktop computer, has an associated owner (e.g. a student who has a personal computer) or caretaker (e.g. a staff member who has a computer in his or her office). For the sake of this policy, owners and caretakers are both referred to as owners.

Owners are responsible for ensuring that their machines meet the relevant security standards and for managing the security of the equipment and the services that run on it. Some departments may assign the responsibility for computer security and maintenance to one or more designees. Therefore, it is possible that one owner manages multiple departmental machines plus his or her own personal computer. Every owner should know who is responsible for maintaining his or her machine(s).

3.4 Security Standards

These security standards apply to all devices that connect to the Conception Abbey network through standard campus ports, through wireless services, and through home and off campus connections.

- Owners must ensure that all computers and other devices capable of running anti-virus software have licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners should update definition files at least once per week.
- Computer owners must install the most recent security patches on the system as soon as practical or as directed by I.T. Services. Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.
- Computer owners of computers that contain sensitive data should apply extra protections. I.T. Services will provide consultations on request to computer owners who would like more information on further security measures. For instance, individuals who are maintaining files with Social Security information or other sensitive personal information should take extra care in managing their equipment and securing it appropriately.

3.5 Centrally-Provided Network-Based Services

I.T. Services is responsible for providing reliable network services for the entire campus. As such, individuals or departments may not run any service which disrupts or interferes with centrally-provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions will be made for personnel in departments who can demonstrate competence with managing the aforementioned services. Also, individuals or departments may not run any service or server which requests from an individual their I.T. Services-maintained password.

3.6 Protection of the Network

I.T. Services routinely scans the Abbey network, looking for vulnerabilities. By connecting a computer or device to the network, you are acknowledging that the network traffic to and from your computer may be scanned.

I.T. Services reserves the right to take necessary steps to contain security exposures to the Abbey and or improper network traffic. I.T. Services will take action to contain devices that exhibit the behaviors indicated below, and allow normal traffic and central services to resume.

- imposing an exceptional load on a campus service;

- exhibiting a pattern of network traffic that disrupts centrally provided services;
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others;
- exhibiting behavior consistent with host compromise;
- exhibiting behavior consistent with illegal activity.

I.T. Services reserves the right to restrict certain types of traffic coming into and across the Abbey network. I.T. Services restricts traffic that is known to cause damage to the network or hosts on it. I.T. Services also may control other types of traffic that consume too much network capacity, such as file-sharing traffic.

Approved by the IT Services Oversight Board 8-05

Acceptable Use Examples

The following scenarios are intended to provide examples of acceptable and unacceptable uses of Conception Abbey's computing resources, based on the Acceptable Use Policy. These examples are not comprehensive but are merely illustrations of some types of acceptable and unacceptable use.

Authorized Use

Acceptable:

- While using someone else's computer from off campus, you remotely connect to the Abbey network to check your email. When you have finished, you log off of your account, closing any browser windows you may have used, and making sure your email password was not saved on the computer.
- While traveling on vacation, you ask a staff person to check your email for you by forwarding your email to their account, removing the forwarding on your return.

Unacceptable:

- While someone else is using a computer, you want to check your email. You ask them to log in, giving them your password to type in for you.
- While traveling on vacation, you ask a staff person to check your email for you by giving them your password.
- A colleague is out sick, and he/she was receiving responses for an event. Rather than calling them at home to ask them to check their email, you attempt to gain access to their account by guessing their password.
- After having your computer hacked, you decide to download and run hacking tools yourself to help your friends out by checking for vulnerabilities on their computers.

Fair Share of Resources

Acceptable:

- You use a shared computer in a Library, computer lab, or departmental cluster that you are authorized to use.

Unacceptable:

- You use your computer connected camera to display what is happening in your room 24 hours a day, 7 days a week on the Internet, and list the site on major search engines and post it on listservers to ensure lots of visitors.
- While using a computer in a departmental cluster, you alter its setup, so that each time it starts up, your favorite programs are started automatically.

Adherence to Laws

Acceptable:

- Taking a CD you own, you make copies of the songs onto your computer so you can listen to them without the CD needing to be in your CD drive.

Unacceptable:

- Taking a CD you own, you make copies of songs onto your computer, and set up sharing to allow others to access those songs from your computer.

Other Inappropriate Activities

Unacceptable:

- While running for political office, you use your Abbey email account to send out email about your candidacy to people who live in your district promoting you as a candidate.
- Using a computer connected to the Abbey's campus network, you establish a commercial business, selling products or services over the Internet.
- Using a computer connected to the Abbey's network, you connect to an outside service where you have hosted your commercial business to upload new files for that business or to download orders.
- You purchase and install a wireless router and attach it to the campus LAN.

Privacy and Personal Rights

Acceptable:

- As part of an investigation into an employee's potential misuse of the campus network for copyright violations, permission is granted from an appropriate office for a supervisor to log into that employee's computer and check files that are stored on it.

Unacceptable:

- While checking the email system for possible problems, a systems staff person has to open a mailbox owned by someone else. In doing so, he or she reads the subject lines, finds one that looks interesting, and opens the email message.

User Compliance

Acceptable:

- When registering for email at Conception Abbey, and finding a policy presented on the screen, an individual reads it and agrees to it before proceeding to the next screen.

- As virus alerts and other news are sent from I.T. Services, an individual takes appropriate action to protect his or her computers from those threats.

Unacceptable:

- When registering for email at Conception Abbey, and finding a policy presented on the screen, an individual quickly clicks on the "I Agree" button without reading the policy or acknowledging responsibility for following it.
- As virus alerts and other news are sent from I.T. Services, an individual sets up an email filter to send the information directly to the trash.

Policy Enforcement

Violation of a computing-related policy may result in disciplinary action, up to and including suspension or termination.

Approved by the IT Services Oversight Board 8-05

Copyright Infringement Policy

Copyright Law, the Illegal Use of File Sharing Programs, Abbey Policies and Procedures for Handling Violations

This document is intended to explain the policies and procedures Conception Abbey follows in responding to notifications of alleged copyright infringements on the campus network.

What is copyright?

Copyright is legal protection of intellectual property, in whatever medium, that is provided for by the laws of the United States to the owners of copyright. Types of works that are covered by copyright law include, but are not limited, to literary, dramatic, musical, artistic, film and multi-media works. Many people understand that printed works such as books and magazine articles are covered by copyright laws but they are not aware that the protection extends into software, digital works, and unpublished works and it covers all forms of a work, including its digital transmission and use.

What is the current law concerning digital copyright?

The Digital Millennium Copyright Act (DMCA), signed into law in 1998, recognizes that digital transmission of works adds complexity to the Copyright Law. The DMCA provides non-profit educational institutions with some protections if individual members of the community violate the law. However, for Conception Abbey to maintain this protection we must expeditiously take down or otherwise block access to infringing material, whenever it is brought to our attention and whether or not the individual who is infringing has received notice.

It is important to note, that the DMCA contains serious implications with respect to infringing activities of faculty, graduate students, or staff who are performing a teaching or research functions if the university has received more than two notices of infringement against an individual within a three-year period.

The Abbey and individuals can be subject to the imposition of substantial damages for copyright infringement incidents relating to the use of the Abbey's network services. In a civil action, the individual infringer may be liable for either actual damages or statutory damages of up to \$30,000 (which may be increased to up to \$150,000 if the court finds the infringement was willful). In addition, individual infringers may be subject to criminal prosecution. Criminal penalties include up to ten years imprisonment depending on the nature of the violation.

Why is it an important issue right now?

Copyright is an issue of particular seriousness because technology makes it easy to copy and transmit protected works over our networks. While Conception Abbey encourages the free flow of ideas, and provides resources such as the network to support this activity, we do so in a manner consistent with all applicable state and federal laws. Conception Abbey does not condone the illegal or inappropriate use of material that is subject to copyright protection and covered by state and federal laws.

What kinds of activities violate the federal law?

Following are some examples of copyright infringement:

- Downloading and sharing MP3 files of music, videos, and games without permission of the copyright owner
- Using corporate logos without permission
- Placing an electronic copy of a standardized test on the department's web site without permission of the copyright owner
- Enhancing a departmental web site with music that is downloaded and artwork that is scanned from a book, all without attribution or permission of the copyright owners
- Scanning a photograph that has been published and using it without permission or attribution as the background of a web site
- Placing a number of full-text articles on a course web page that is not password protected, therefore, the web page is accessible to anyone who can access the Internet
- Downloading licensed software from non-authorized sites without the permission of the copyright or license holder
- Making a movie file or a large segment of a movie available on a web site without permission of the copyright owner

Specifically, is sharing and downloading MP3 files and videos illegal?

It is true that some copyright holders give official permission to download MP3 files and you might be able to find a limited number of videos that are not copyright protected. It is also true that some MP3 files are copyright free and some MP3 files can be legally obtained through subscription services. However, most MP3 and video files that are shared do not fall into any of these categories.

US Copyright Law allows you to create MP3s only for the songs to which you already have rights; that usually means you purchased the CD or tape. And US Copyright Law allows you to make a copy of a purchased file only for your personal use. Personal use does not mean that you can give a copy to other people, or sell a copy of it.

How do you get caught violating copyright law?

Copyright holders represented by organizations such as the Recording Industry Association of America, the Business Software Association, and the Motion Picture Association of America are applying serious efforts to stop the infringing downloads of copyrighted music, movies, and software. The companies or their agents locate possible copyright infringements by using automated systems, or "bots" that search the networks looking to see if any of the common music, movie or software sharing programs are active on a port (e.g. KaZaA, Gnutella). The bot then asks the sharing program if it has a music title by a particular artist. If the sharing program answers positively, the bot reports the particular IP address and title to an authority, who then sends out the violation notices to the owners of the IP address.

Conception Abbey's network has a range of IP addresses and all computers connected to the campus network have an IP address. When we get a violation notice, I.T. Services locates the IP address and whenever possible, the user of that address. At that point, the Abbey is required to act on the notification.

If the IP address leads to my computer, what happens next?

These notices come to the Director of IT Services from organizations that represent the artists and copyright holders. When the Abbey receives such a notice, staff in I.T. Services look up the network IP address and stop network services to the port that is connected to the computer where the infringing material resides. At this point, the computer cannot use any Abbey resources or Internet resources. Once the identity of the individual is known, they are notified that they must remove the infringing material from their computer and inform I.T. Services of its removal before network access will be reinstated.

Notifications: If this is the first notification that the Abbey has received on an individual, I.T. Services will verify that the infringing material has been removed from the computer. Once this is done, the network connection will be reinstated and the computer can return to the network. A report about the violation of copyright will be sent by I.T. Services to the business office. Any further violations will be handled within the bounds of the Abbey's disciplinary process.

Approved by the IT Services Oversight Board 8-05

Telecommunications Policy

1.0 Purpose

The purpose of this policy is to define appropriate use of telephone services at Conception Abbey.

2.0 Scope

This policy applies to all telephone services provided by Conception Abbey including all telephony originating from and terminating at the Abbey telecommunications system. Use of the system is governed by the Conception Abbey Acceptable Use Policy.

3.0 Policy

3.1 Prohibited Calls

- 900 Type Calls - These calls are prohibited
- Collect Calls - Receipt of these calls through the use of a Abbey phone is prohibited.

3.2 Personal Telephone Use

Access and use of Abbey-provided devices is a privilege that is granted in connection with an individual's duties to the Abbey and are to be used for the conduct of approved Abbey business and/or in furtherance of the educational mission of the Seminary.

The use of Abbey phones for personal calls is not allowed outside those placed with calling card services or billed to your personal telephone account. Personal Authorization Codes are provided at a users request for the purpose of placing personal telephone calls. Users are expected to reimburse the Abbey for all calls appearing on their telephone billing statement no later than 30 days after the billing period. Billing disputes may be presented to the business office.

3.3 Review of Phone Use

Departmental management is responsible for determining what telephone devices are needed to conduct Abbey business (including but not limited to cell phones, wireless-enabled Personal Digital Assistants, and pagers) and what the appropriate service level and billing plan should be for these devices.

Departmental management is also responsible for regularly reviewing monthly telephone billing statements and for investigating unusual calling patterns, unexpected charges or unusual call volume. The I.T. Services will provide consulting and advisory services upon request to assist in clarifying usage questions.

3.4 Privacy in Telephone Services

Conception Abbey phones and services may be monitored for maintenance purposes.

Cellular transmissions are not secure, so employees should use discretion in relaying confidential information via these devices.