

Policy on Responsible Use of Technology

Responsible Department: Calvin Information Technology
Approval History Policy Statement -- Information Services Committee on July 1, 1993 as a guideline Policy Statement and Appendix A -- Information Services Committee on July 8, 2005 as a policy -- Cabinet, July 15, 2005 as a policy Policy Statement and Appendices A and B -- Information Services Committee on May 12, 2006 -- Cabinet on July 19, 2006 -- Planning and Priorities Committee on October 19, 2006 -- Faculty Senate on November 6, 2006 -- Information Services Committee, editorial revision to Appendix A, January 12, 2007 -- Board of Trustees February 9, 2007 Appendix C added -- Information Services Committee on May 9, 2008 -- Cabinet on August 13, 2008 -- Planning & Priorities Committee December 19, 2008 -- Faculty Senate March 2, 2009 -- Board of Trustees May 22, 2009
Revision/Review History Summer 2005 rewritten as a policy with Appendix A May 2006 reviewed and Appendix B added August 2007 reviewed May 2008 reviewed and Appendix C added
Where is this policy published? CIT Web Pages Staff Handbook Student Conduct Code – Appendix F Faculty Handbook
The VP for Administration, Finance & Information Services and the Dean of Judicial Affairs have the authority to modify examples as appropriate.

Policy Overview

"Grateful for the advances in science and technology, we make careful use of their products, on guard against idolatry and harmful research, and careful to use them in ways that answer to God's demands to love our neighbor and to care for the earth and its creatures." (*Paragraph 52, Our World Belongs to God, CRC Publications, 1988.*)

As a community that yields to the leadership of Jesus Christ, Calvin College expects responsible use of technology by enfranchised users of Calvin information technology resources. This policy was created to amplify what this community intends by responsible use.

This policy defines responsible use as regards to:

- Respect for one another's need for access

- Respect for one another's values and feelings
 - Respect for one another's property
 - Respect for one another's privacy
 - The stewardly use of the college's information technologies
 - Respect for the ownership, right to use, and protection of information
-

Scope

This policy applies to all enfranchised users of Calvin information technology resources. An enfranchised user is anyone who has been given permission to use Calvin information technology resources.

Consequences for Policy Violations

Use of information technology resources at Calvin College is a privilege, not a right. Violation of any part of this policy will subject the violator to disciplinary action, which may include any of the following: warning, loss of access, or referral to the appropriate judicial body.

- Students: A breach of any part of this policy may warrant referral to the Senior Judicial Advisor or Judicial Advisor as defined in Appendix G of the "Student Handbook: General Disciplinary Process"
- Staff: A breach of any part of this policy may warrant referral to their immediate supervisor as addressed in "The Staff Handbook" section on Rules of Conduct and Working Relationships
- Faculty: A breach of any part of this policy may warrant referral to the Provost's Office as addressed in section 6.1 of the "Faculty Handbook: Procedures for Addressing Allegations of Misconduct"
- Alumni and guests of the college: A breach of any part of this policy may warrant suspension or permanent termination of access to Calvin information technology resources

Any violation or suspected violation of this policy should be reported to one of the Information Technology Directors or the VP for Administration, Finance, & Information Services.

Policy

Respect for one another's need for access

Calvin College is a community where all members are expected to act in their neighbor's best interest. No enfranchised user may appropriate information technology resources that interfere with the educational, research, or service activities of the college or the administration thereof.

Examples of technology appropriation which do not respect one another's need for access include but are not limited to:

- Anything that negatively affects the college's network bandwidth (e.g., running any program that generates a large volume of network traffic)
- Destruction or potential destruction of resources by the use, ownership, or distribution of viruses, worms, Trojan horses, spam, spyware, chain email or other destructive programs

Respect for one another's values and feelings

New technologies often increase our ability to communicate as well as miscommunicate. That communication should demonstrate respect for others and a sense of personal integrity. Ephesians 4:29 is applicable here: "Do not let any unwholesome talk come out of your mouths, but only what is helpful for building others up according to their needs, that it may benefit those who listen." Thus, communication that degrades or harasses individuals or groups is unacceptable.

The need to communicate with respect and integrity is particularly important in our contacts with those outside of Calvin College. Our communications will reflect not only on the college but also on our witness as Christians.

Examples of technology use that do not respect one another's values and feelings include but are not limited to:

- Messages that intimidate, harass, threaten or embarrass (e.g., email, IM, voicemail, web pages, web logs)
- Any use of web life (Facebook, MySpace, etc.) that is contradictory to the principles of the college codes of conduct (*Faculty Handbook* – Chapter 6, *Staff Handbook* – Section D, *Student Code of Conduct*).

Respect for one another's property

Theft or unauthorized use of tangible property, intellectual property, college data, or college information technology resources will not be tolerated. Such theft is both unethical and illegal, and can subject both the individual as well as the college to prosecution.

Examples of technology use that do not respect one another's property include but are not limited to:

- Unauthorized copying of copyrighted software (software piracy), documents, and intellectual property including music and movies
- Unauthorized access of someone else's account
- Unauthorized access of any of the college's information technology resources
- The unauthorized sending of messages or publishing of information under someone else's username
- Using college information technology resources for illegal, commercial, profit-making, or any other purposes other than those approved by the college
- Granting access to the college's information technology resources to non-enfranchised users (e.g., giving out your passphrase so an unenfranchised user can access the college's information technology resources)
- Use of unauthorized software or devices on the college network that bypass the college's network security, interfere with the operations of the college network or provide unauthorized services on the network. (e.g., switches, hubs, repeaters, wireless access points, modems) For additional clarification, please see Appendix A: Statement on Wireless Networking Devices.

Respect for one another's privacy

Respect for others also means a respect for their privacy. Any unauthorized access to other's files, electronic mail, voicemail or other communications is not permitted. Likewise, unauthorized access into restricted system files is not permitted.

Examples of technology use that do not respect one another's privacy include but are not limited to:

- Unauthorized tapping of telephones or network transmissions including wireless transmission (e.g., running network sniffers, keystroke loggers)
- Obtaining, possessing, using, or attempting to use someone else's passphrase, PIN, PAC, voicemail ID or other electronic communications

The stewardly use of the college's information technologies

We are stewards of technology; therefore God requires accountability in our use of these gifts.

Examples of technology use that do not represent a stewardly use of the college's information technologies include but are not limited to:

- Using large amounts of fileserver space. (e.g., storing a large number of personal mp3s, digital images, etc. that do not pertain to the educational, research, or service activities of the college or the administration thereof)
- Misuse of printers and printer supplies. (e.g., printing extensive source materials such as entire chapters of books, taking paper from labs for personal use)
- Misuse of email. (e.g., sending email to the entire campus for any purpose including spam, spyware, chain email, etc.)
- Unsolicited mass mailings to individual email addresses. (e.g., advertising for events or activities, or "non-personalized" surveys.) These mailings should use established Calvin mailing lists.
- The removal of CIT-approved management client software on College-owned resources or the renaming of a computer that is owned by Calvin College. (See [Appendix C: CIT Management of Calvin-owned information technology resources](#))

Respect for the ownership, right to use, and protection of information

As a community of individuals, Calvin College strives to balance an individual's right to personal privacy against the community's need to collect information for accountability, assessment, security, and other purposes. Calvin College classifies information using the following categories:

- **Sensitive information:** Information in this category may not be distributed without consideration of its sensitive nature. (See **Appendix B: Information Security: Ownership, Right to Use and Protection of Information**)
 - **Private information** is personal information, including personal intellectual property, which is accessible only by its owner and those to whom they entrust it, except under exceptional circumstances.
 - **Confidential information** is institutional information normally handled in the same manner as private information, but may be accessed by other authorized members of the College community under limited additional circumstances.
 - **Community information** is institutional information that is intended for distribution within the College community.
- **Public Information:** Information in this category is distributed without restriction. (See **Appendix B: Information Security: Ownership, Right to Use and Protection of Information**)

Examples of technology use that do not respect the ownership, right to use, and protection of information include but are not limited to:

The transfer of ownership and/or granting access to your personal information technology

accounts. Individual technology accounts are for the exclusive use of their owners.

- You may not share your passphrase, log in for another user or in any way grant access to your IT accounts.
- Calvin employees (faculty, staff, and student employees) may not be required to share their username and passphrases as a part of the normal course of business operations.
- You may, however, grant access to your files, your computer or grant remote control access to CIT support personnel if you have requested assistance in solving a hardware or software problem. (See [Appendix C: CIT Management of Calvin-owned information technology resources](#))

Faculty staff and students should observe the appropriate safeguards to protect access to sensitive information. (See **Appendix B: Information Security: Ownership, Right to Use and Protection of Information**).

Appendix A: Statement on Wireless Networking Devices

Purpose

Managing the deployment and configuration of wireless networking devices on Calvin's campus is necessary to prevent unauthorized or insecure use of Calvin's data network and to prevent the conflicting use of the unlicensed radio frequency spectrum.

Two specific issues need to be addressed by Calvin Information Technology (CIT) in the management of a wireless environment:

1. Since there are a limited number of wireless networking channels available in the 2.4 GHz and 5 GHz unlicensed frequency ranges in which many wireless devices operate, and since this range is also shared with other devices such as cordless phones, CIT needs to make sure that wireless devices do not conflict with one another. This means that CIT needs to manage which networking channels are in use and where wireless devices are located.
2. It is the responsibility of CIT to control access to our campus network. Allowing unencrypted and unauthenticated access through a wireless access point constitutes an opportunity for a significant security breach in our campus network.

Wireless implementation on Calvin's campus:

1. All authorized wireless access points on campus will be purchased and installed by CIT.
2. The location of authorized wireless access points on campus will be determined by the Network Operations Center of CIT in consultation with academic and administrative departments, the Information Services Committee, and Faculty Senate.
3. CIT reserves the right to disconnect any access point which is not part of the CIT deployed wireless network and may require the discontinued use of any other device, such as cordless phones or microwave ovens, etc. which interfere with that wireless network.
4. There are occasions when groups have a legitimate need to wireless access in areas not covered by the authorized wireless network. In such cases, wireless access points may be set up with the permission of CIT, but the maintenance and configuration of these would not be the responsibility of CIT. If they are deemed problematic, they are to be removed at the request of CIT.

Appendix B: Information Security: Ownership, Right to Use and Protection of Information

A. Purpose

Calvin College strives to balance an individual's right to personal privacy against the community's need to collect information for accountability, assessment, security, and other purposes. This document defines the details that govern the ownership, right-to-use, and protection of information at Calvin College.

B. Information Ownership Definitions

Generally speaking, Calvin College categorizes the information it gathers during the normal course of institutional operation into two categories:

1. **Sensitive information:** Information in this category may not be distributed without consideration of its sensitive nature.
 - **Private information** is personal information, including personal intellectual property, which is accessible only by its owner and those to whom the owner directly entrusts it, except under exceptional circumstances.
 - **Confidential information** is institutional information normally handled in the same manner as private information, but may be accessed by other authorized members of the College community under limited additional circumstances.
 - **Community information** is institutional information that is intended for distribution within the College community.
2. **Public Information:** Information in this category is distributed without restriction.

C. Information Ownership Examples

1. Private information

Members of the Calvin College community have access to information technology (IT) equipment, including but not limited to computers, the college network including their personal file space, computer-related equipment, telecommunications equipment, and associated infrastructure. The College will treat information created by individuals on such equipment within the areas specifically assigned to the individual as *private* information.

Examples of *private* information include:

- Information stored on personally owned computers, such as files containing personal correspondence, homework assignments, etc. are considered *private* information, even when those computers are operated on Calvin's campus.
- Information stored on the hard drive of College-owned computers is considered private. Please be aware that unless these files are stored in an encrypted format they are readily accessible to anyone else that logs into that computer.
- Personal information stored on the College network in storage space specifically assigned to the person will be considered *private*. (e.g. your home drive, email, voicemail) Files stored on the network in public locations are not considered private. (e.g. your department's common drive or legacy\users\common)

NOTE: Staff or faculty member who leave the college forfeit ownership to any files remaining on any personal space on the college network or on any Calvin-owned

computer hard-drive. These files will then be considered to be *confidential* property of the college.

2. Confidential information

During the course of its normal day-to-day operation, the College records information about individuals. The College will treat such information as *confidential*.

Examples of confidential information include:

- Personnel records such as social security number, personal account and financial transaction information and academic records, such as academic transcripts, class registration lists, employment histories, teaching evaluations, demographic information, etc. As an educational institution and employer, the College must collect and maintain information regarding its students, employees, alumni, and prospective students. Calvin maintains a policy of confidentiality and non-disclosure with respect to this personal information.
- Academic records of current and former students regardless of their age or status in regard to parental dependency are protected under the Family Educational Rights and Privacy Act (FERPA) of 1974. The Calvin Registrar's office holds the responsibility for implementation of FERPA at Calvin. This information is published in the college catalog and on the Registrar's Office website (<http://www.calvin.edu/admin/registrar/ferpa.htm>).
- Information that is provided incidentally, such as phone records, office records, Campus Store purchase records, ID card reader records, etc.; or information that is provided voluntarily, such as membership in a campus organization, participation in campus studies or surveys, etc. Permission to divulge such information should not be required to use campus facilities, access campus resources, join campus organizations, participate in campus studies, etc.
- Information that is provided incidentally by anyone who accesses Calvin's network resources that may automatically and unknowingly generate information about themselves and their habits (e.g., web-page access logs, in-transit user-passphrases, network packets, etc.). To ensure that college resources are used appropriately, various software and hardware tools may be used by the Calvin Information Technology department (CIT) to monitor Calvin owned or operated communications systems, computing resources and/or files. This may include log analysis tools, or tracking software to help CIT report trends and errors on college websites or equipment.

Note: Voluntarily-provided or incidentally-collected information will be presumed to be *confidential* unless prominently noted otherwise.

3. Community Information

As a community of individuals, the College must balance its individuals' rights to personal privacy against the needs of the community. Wherever possible, the College will strive to provide individuals with control over their own personal information. However this right must be balanced with the right of the members of the community to access information that affects them, and the need for the community to be able to disseminate important information to its constituents quickly and efficiently. *Community* information is thus an intermediate information category falling between *confidential* and *public*.

Examples of *community* information include:

- Information intended for on-campus distribution only, such as messages sent to campus listservs, outcomes of campus studies, community directory information (*Names and Faces, PeopleSearch*), etc. Community directory information includes a community member's address, telephone number, or likeness when linked to the member's name or other personal identity information.

Note: Care should be taken when giving a person's community directory information to someone outside the College community.

4. Public Information

Information that is not considered "sensitive" will be treated as public information.

Examples of *public* information include:

- Information the college collects for public dissemination, such as faculty annual reports, information for the campus yearbook (Prism), information for the campus newspaper (the Chimes), likenesses not linked to personal identity information (for brochures or other public relations purposes), etc.
- Information accessible via the World Wide Web from Calvin College servers, such as personal web pages, department web pages, etc.

Note: Calvin College web pages are governed by the *Calvin College Web Policy* (<http://www.calvin.edu/admin/webmanager/policy/>). As stated in this policy: "... [the College] will periodically monitor College-sponsored web pages for quality and identity issues. It will not review student organization or personal home pages. If alerted to objectionable pages by another source, [the College] will discuss the page and may either make a contact with the person responsible or decide to refer to the proper campus judicial body."

D. The Right to Use information

1. Private Information

Members of the college community will access private information only with verbal or written authorization by the person owning the information or by written authorization from the College's Vice President for Information Services and one other officer of the college. Written authorization may be requested:

- to comply with a judicial order or subpoena.
- in the event of accusation of academic dishonesty.
- in the event of a health or safety emergency.
- in the event of a request by Federal, State, and local authorities involving an audit or evaluation of compliance with education programs or employment law.
- in the course of investigating abnormal system performance, a security breach, or abuse of IT resources, as defined in the College's *Policy on the Responsible Use of Technology*.

Information gathered by tracking software or log analysis tools may be used to help in tracing unusual trends or suspicious computer activity. To protect the security, safety and welfare of the college and its resources, authorized CIT employees may need to use this data to access or examine the contents of normally private files and/or information.

2. Confidential Information

Authorized personnel may access confidential information under the circumstances governing access to private information, plus the following additional circumstances:

- to comply with the Family Educational Rights and Privacy Act (FERPA)

- to comply with a request by an organization conducting studies on behalf of educational institutions. An individual's personally identifiable information will not be released without the permission of that individual.
- in the performance of their responsibilities in their position as a college employee.

Note: Non-academic confidential information will not be released to parties outside of the College, except for information necessary to maintain the affiliation of the College with the Christian Reformed Church (CRC) and its associated organizations.

3. Community information

Whether to safeguard intellectual property, ensure the integrity of the educational process, or for other reasons that benefit the community, the College supports information distribution that is limited to members of the College community.

- Access to community information in electronic format will be restricted via IP address or user-authentication, such as information available to non-guest users of KnightVision, the Hekman Digital Library, online evaluation systems, and web-pages containing community information.
- When collecting information that will be distributed to the campus community, the collection tool (e.g., form, information sheet, web page, etc.) should indicate this prominently.

Sample statement: *This information will be distributed to the campus community.*

Note:

- Individuals should be aware that while some information may be intended for the *community*, such information can easily become *public*, since the College is unable to prevent the dissemination of such information outside of the campus community.
- Because the College cannot enforce the containment of community information in hard copy and other portable formats individuals should exercise caution and restraint when releasing personal information to the *community* category.

4. Public information

The College regularly requests information from faculty, staff, students and prospective students for the purpose of publication.

- The College is free to release such public information as it sees fit, via print, electronic, or other media. When requesting such *public* information, the collection tool (e.g., form, information sheet, web page, etc.) should indicate prominently that the information is for publication.

Sample statement: *The information requested here is for publication.*

E. Protecting confidential information on electronic devices

1. All electronic records containing Calvin College confidential information must be stored in a secure fashion against unauthorized access.
2. Confidential information stored on any portable electronic medium (e.g., laptop, CD, DVD, USB drive, "thumb drive", etc.), even for temporary use, must be stored in a secure fashion against unauthorized access using an appropriate technology prescribed by CIT. Please contact the CIT HelpDesk for additional information or assistance.
3. If you have access to confidential information and you must leave your desk you must secure your computer from unauthorized access.

Example: Turn on a password-protected screen saver, lock the workstation, or shut down the computer.

4. Electronic records containing confidential information that are stored on Calvin's computer network must be stored in a "secure" location that is accessible only by those authorized to view the information.
Example: Store confidential information on your home drive or another network location where access is restricted by passphrase to those authorized to access the information.
5. Persons with access to Colleague, Benefactor, or other electronic systems containing confidential information must take reasonable care to minimize the time that their computer screen displays the information. They must also take reasonable precautions to shield their computer screen from displaying this information from those without a legitimate work-related reason to view the confidential information. Computer screens displaying confidential information should never be left unattended.
6. Appropriate procedures will be followed to remove confidential information when computers or electronic media containing confidential information are disposed of or redeployed.

F. Protecting Printed Confidential Information

1. Persons finding it necessary to print a file containing confidential information must take reasonable efforts to ensure that unauthorized users do not have access to the information. This includes printing to printers not accessible to the general public and minimizing the time the file is left on the printer.
2. All paper documents containing confidential information should be destroyed in an appropriate manner.

G. Protecting Confidential Information on the Campus Network or over the Internet

1. Calvin will not require individuals to send confidential information to the College over the Internet or by email, unless the connection is secure or the confidential information is encrypted.
2. Confidential information must not be sent over the Internet or by email unless the connection is secure or the confidential information is encrypted.

H. Adjudication of Future Cases

The preceding sections provide a framework within which particular kinds of information can be categorized. For each category, it also offers specific cases that illustrate the kinds of information that fall within that category.

Given the changing nature of information services, new and unanticipated cases will undoubtedly arise. In such circumstances, the given cases are intended to serve as guidelines by which new cases can be positioned within the framework.

It is possible (and even likely) that different people will disagree on the placement of a new case within the framework. In such situations, the case will be brought to the College's *Information Services Committee* for adjudication.

Appendix C: CIT Management of Calvin-owned computers

A. Purpose

Centralized management by CIT of the deployment and management of Calvin computers is necessary to ensure the security of both personal and college data and to aid in compliance with government and industry requirements and regulations.

B. Computer deployment

1. Calvin-owned computers are configured and deployed with CIT-approved management client software installed as appropriate for their operating systems and hardware configurations.
2. This software performs functions including, but not limited to, application deployment, configuration management, inventory, antivirus and antispyware, patch deployment, encryption, and remote support. These management clients are an essential component of a secure, manageable, efficient, and supportable computing infrastructure for users of Calvin College computing facilities. As such, CIT is obligated to install and maintain these management clients on all Calvin owned computers.

C. Removal of management clients

1. Management clients may not be removed except by authorized CIT personnel or with written permission from CIT's Security Officer or his/her designee.
2. Additionally, to aid in the correct function of management clients, each computer owned by the college will be assigned a computer name by CIT which may not be modified by users.

D. Protecting the privacy of Calvin community members

1. One function of the management clients is the ability of support staff to remotely view and remotely control Calvin-owned information technology workstations.
2. To protect the privacy and security of Calvin's community members, remote access requires explicit approval of the user logged in to the workstation prior to support staff remotely viewing or remotely controlling the workstation.
3. Users, whose workstations are being remote controlled will, at all times, be allowed to view the actions of support personnel. If the user chooses to leave his or her workstation during the remote access or remote control, they should first inform the support staff and give explicit approval for remote access/remote control to continue.
4. Public use computers may be remote controlled when no one is logged in to the machine.
5. Several Calvin computer classrooms use classroom computer management software. This software is designed to allow the instructor to supervise the work being done on each workstation, take control of the workstations, share any workstation's desktop with the rest of the class, block access to web browsing, and manage the individual workstations. The use of this kind of classroom management software is exempt from items D. 2 and D. 3 of this appendix provided those who are logged in to the computers have been notified that classroom computer management software is being used.