GORDON
COLLEGE

Responsible Use of Computers Policy

Gordon's computer network extends the capability of people on campus to find, collect, create, analyze, display and communicate all kinds of information. Likewise, it extends ease of access, advantage for the technically gifted, and some anonymity, all of which can test moral conviction and personal restraint. The result is a range of practical challenges to our Statement of Life and Conduct. These include issues of stewardship, forbearance, concern for others, theft, dishonesty, immodesty, adherence to law, submission to proper authority and even discerning the worldly spirit of the age.

How we use computers at Gordon is a telling test of our Christian character in a community activity involving personal responsibility. What is involved is more a privilege than a right. As people use computers and the network at Gordon, the College expects they will do so in ways that are not only lawful and ethical but responsible and courteous as well. That requires respect be given to the principles and particular examples set forth below.

Those using computers at the College must be aware that to enter the public Internet is to risk encountering materials and behaviors they may find offensive. It is impossible for the College to shield its users from such things. As the College deals with this issue, it is committed to avoiding the kind of censorship inimical to an academic community; at the same time it seeks to draw upon the commitment made by its faculty, staff and students to its distinctively Christian standards. The purpose of this policy is to alert computer users at the College to the potential temptations and dangers inherent in such use, to outline the College's position on these issues and to state the need for personal diligence in adhering to standards of Christian conduct. The policy also states the right of the College to restrict the use of its computers and network in response to violations of this policy or state and federal laws.

RESPECT FOR PRIVACY, SECURITY AND THE INTEGRITY OF INFORMATION

Computer hardware, networks, software, user accounts and the data they contain all belong to somebody. The fact that technology sometimes makes it easier for individuals other than the owner to access these things does not make it right to do so. In general, using, accessing, altering or removing computer equipment, accounts or data for which one does not have explicit ownership or right of access is unethical, and possibly illegal.

Specific examples:

- The College controls access to its shared systems by the assignment of accounts. Recipients are expected to protect their assigned accounts by proper use of a password. They may not grant anyone else access to that account or share their password.
- Attempted or actual access to any account or data not personally owned is unacceptable, regardless of intent and whether or not the material is protected. The only exceptions are for access specifically authorized or assigned by the owner.
- The College reserves the right to inspect the contents of all accounts and files on computers directly connected to its network in the course of maintenance, compliance with contractual requirements or investigation of suspected violations of the Responsible Use of Technology policy. Such access will be done with regard for privacy and confidentiality. When appropriate and possible, cooperation of the user will be sought first.
- Providing information or other means of access that encourages or enables use of the College's network and computers attached to it by anyone not a current faculty member, staff member or student of the College is unacceptable.
- Knowingly loading, creating or downloading software concealing a virus or other detrimental code and running such software on the College's network or attached computers is unacceptable.
- Any use of the College's network or computers attached to it to develop or distribute harmful software or gain improper access to or make improper use of computer systems elsewhere is unacceptable.
- Access to data contained in the College's administrative systems is limited to faculty and staff who have a particular need for that information in pursuit of their responsibilities, and as appropriate to the student to whom the records pertain in accordance with provisions of the Family Educational Rights and Privacy Act. The College does not divulge information of any faculty member, staff member or student to parties lacking explicit legal entitlement to it.
- The College makes a concerted effort to keep its systems and data secure. Today's technology, however, does not provide total guarantee of privacy for any electronic data. For example, the College keeps extra copies of all

server data in the routine process of protective backup; deletion of online files by a user does not mean that no other copy remains. All users are advised to exercise careful judgment regarding information or messages they enter into the College's network and the computers attached to it.

RESPECT FOR OWNERSHIP AND COPYRIGHT

All of the computer and network hardware purchased by the College for use of faculty, staff and students remains its property. With two exceptions, the material contained in those systems, particularly what resides in its administrative computers, is also the property of the College. One exception to this ownership is software which remains the property of third parties while used by the College under the provisions of licenses and copyrights. The other exception is material collected or created by users for which they have rights of authorship. The College honors and operates within the provisions of such ownership; it expects all who use its computers to do likewise.

Specific examples:

- Users should always assume that material on the College's network, the computers attached to it, or on the Internet are copyrighted or the property of others unless explicitly labeled otherwise. Keeping, copying, sharing or distributing software, images or other tangible or intellectual property which one does not own, does not have a valid license for or is in violation of copyright, are all unacceptable. No such improperly gained material is to reside on the College network or the computers attached to it; if discovered it will be removed.
- The College's computers and network are intended only for the use of current faculty, staff and students unless explicitly designated otherwise. Such use is meant for the purposes of regular academic life. Personal use must be constrained to what is reasonable and will always be given lowest priority.
- Use of the College's computers or network exclusively for third parties is unacceptable.
- Hardware (with the exception of laptop computers), networks and software owned or under license by the College are not to be moved, removed or altered except by members of its information technology staff.

RESPECT FOR RESOURCES

The College intends its computers and network to serve as a support for the widest possible number of its people and activities. They are a resource which is both shared and finite. Their use by any constituency must be reasonable with regard to its impact on all other users.

Specific examples:

- Where conflicts of resources arise, priority will be given to academic and administrative work over all other uses.
- All users are expected to show regard for the resource by routinely removing duplicate or unnecessary files, or seeking off-line means of storage.
- Knowingly running programs or tasks which seriously degrade the performance of College computers or networks is unacceptable. Bandwidth intensive activities such as network-based games, peer-to-peer services or talk sessions will usually be given very restricted network resources and may at times be disallowed at the College's discretion.
- All personally owned computers brought to campus will not be allowed to plug into the campus network until they have been tested and certified by a member of the information technology staff to be clean of viruses and to have the then current levels of security provisions installed for both their operating system and the College-required anti-virus software. The College reserves the right to automatically update via the network by the security provisions appropriate for the operating system and anti-virus software of all computers attached to its network.
- Once allowed on the network, if it is determined that for failure to keep current with operating system and anti-virus software patches and updates, an individual computer is infecting and continues to re-infect the campus network with a computer virus, network access from that computer will be suspended for at least a week, and a fee will be charged. Only after that computer has been tested and certified by a member of the information technology staff to be free of computer viruses, that virus protection software is active, and that virus protection definition files are up-to-date and all current security updates have been applied, will network connectivity be reestablished.
- Generating chain letters or sending broadcast messages beyond what the College provides through list serves and distribution lists is unacceptable.
- In public computer areas such as labs, installing software not owned by the College and leaving personal files on internal disks are unacceptable. College staff will routinely remove all such materials from public machines without notice.
- Unnecessary paper printouts are a serious resource waste, and all users are expected to consciously save paper.
- Setting up on the College's network servers not owned and operated by the College is unacceptable. This does not extend to the routine ability of personal computers to have shared files and folders open for reasonable access and use. It does pertain, however, to things like Web servers and peer-to-peer servers which offer general

services to the public. Peer-to peer servers designed to offer copyrighted music and video materials are not acceptable and will be blocked and/or removed by information technology staff.

- Using on campus or in connection with the campus network any hubs, switches, routers, wireless access points or other devices for extending or managing Ethernet networks not owned by the College and managed by information technology or other approved staff, is not acceptable.

RESPECT FOR COMMUNITY

Technology has the appearance of impersonality, but in almost every instance computers and networks are being used by people. As these things are shared within the College, there is a need to retain the sensitivity and care which are expected of all interpersonal communication.

Specific examples:

- The creation and sending of email or other messages which are harassing, degrading, libelous or otherwise harmful is unacceptable.
- The creation and sending of email or other messages which conceal the author's identity or that are represented as being from someone or someplace else is unacceptable.
- Some of the material available in the software market and Internet is at odds with the standards embraced by Gordon's Christian community. Any use of the College's network or the computers connected to it to handle such material, be it racist, pornographic or otherwise harmful to the people and spirit of this community, is unacceptable. It is the College's policy and practice to block access to websites known to be pornographic or racist.
- Using the College's network or the computers connected to it to inhibit or interfere with the work of others is unacceptable.
- Modifying the setup or contents of public computers like those in labs is a severe inconvenience to subsequent users and is unacceptable.
- Use of another's ID, username or password to access private information or in any way altering the academic or administrative data of others is unacceptable.

RESPECT FOR ORDER

The free and advantageous use of the network and computers connected to it requires a responsible use policy to be followed by all, and violations of this policy will be addressed. The guiding principle will be that use of these resources is not an individual right but a privilege that must conform to Gordon's Christian standards.

Specific examples:

- The College may in its discretion take such actions in response to violations of this policy as it deems appropriate. These include investigation and confrontation of violators, suspension of privilege, referral to the judicial process or legal action.
- The College disclaims responsibility for any loss of electronic data which may occur in the course of its efforts to preserve the security and proper operation of its computer systems and network, or to assure compliance with this policy.
- It is the position of the College that users of its systems bear responsibility for their own online conduct and content. The College will not be held responsible for defending its users against litigation which arises from conduct or content which violates College policy.

PORNOGRAPHY

Gordon College provides access to the Internet through an extensive computer network with ports in each residence room. There is a broad range of material accessible through the Internet, including things like pornography that are not in keeping with biblical standards of holiness. The College has blocking measures in place for such things as pornographic or hate speech sites on the Internet. However, such measures cannot ensure that all materials of this type are effectively blocked, and it is therefore vital that Gordon College students exercise discernment and seek to act in accordance with biblical standards while using the Internet. Misuse of the computer systems may result in the loss of computer-access privileges as well as other disciplinary action. The possession or viewing of pornographic materials in any form is prohibited.