

Terms and Conditions for Computer Accounts / Usage

Acceptable Use Policy

0.0 Highlights

The following summarizes major points. Please read the entire document.

0.1 Your computer and email accounts may be used for:

- curricular and academic activities
- email and access to Worldwide Web pages

Your account may *not* be used:

- by family members, friends, classmates or colleagues
- for commercial or business purposes
- for any activity prohibited by law
- to access sexually explicit or pornographic materials

Your account may be suspended or terminated, and other disciplinary action taken, for:

- violating policies in these *Terms and Conditions*
- using it for commercial or business purposes
- allowing others to use your account
- accessing sexually explicit or pornographic materials
- transmitting, using or serving unauthorized software
- violating copyrights for documents, media or software
- computer tampering

You are expected to use your College email account for all email communication with College offices and officials.

0.2 Faculty, Staff, or Students who wish to connect their personal computers to the campus network must be able to demonstrate that steps have been taken to protect against known vulnerabilities (see Section 12 for details).

0.3 ResNet users or other persons granted permission to connect a personal computer to the campus network are subject to all of the terms and conditions in this document.

1.0 General Information

Wheaton College provides computing and network services for employees and currently registered students, on servers and networks owned and operated by the College. The College reserves the right to circumscribe operation of these facilities, using policies consistent with its mission and the role computers and networks are intended to play within that mission. Specifically, each person's conduct in the use of such services is expected to be consistent with and conform to policies set forth herein, as well as in the College's *Community Covenant*.

In any given academic term, student computing and email accounts are granted only to students who are officially registered for that term.

We trust that all who use the College network and associated computer systems will behave in ways that demonstrate convincingly to the world that we are a *community seeking to honor Christ and His Kingdom in all we do*.

2.0 Computer Accounts

Students and employees can use College-owned systems only by obtaining "accounts" for these systems. These are accessed using a *username* (also called a *login name*) and password. Only the person to whom the account is assigned is authorized to use it; the password is intended to ensure this. To allow friends, classmates, parents, spouse, children, colleagues, or anyone else to use one's account is to violate the Acceptable

Use Policy. If students or employees let other people use their accounts, they and the person using the account are in violation of College policy, and subject to disciplinary action.

2.1 Faculty and Staff apply for accounts by submitting a completed and signed *Computer Account Application* form, either printed from the Intranet web page or obtained from Computing Services. The signed form indicates that the employee has read these *Terms and Conditions* and pledges to abide by the policies contained therein. Each year user accounts are renewed, by the user signing and returning the current version of this form.

2.2 Students are granted accounts when they matriculate, and these accounts are activated in time for their arrival on campus. Upon arrival students must sign and return a *Telephone and Computing Services Policy Acknowledgement* form. The signed form indicates (among other things) that the student has read these *Terms and Conditions* and pledges to abide by the policies contained therein.

Students who leave school and return in a later term are required to sign and return a *Telephone and Computing Services Policy Acknowledgement* form as part of the re-admission process.

3.0 The Campus Network

Many computers connect to the campus network, those owned and operated by the College as well as personal computers brought by students and faculty. The network provides a gateway to the Internet, as well as access to other networks and computer systems not owned or operated by the College. Users of the campus network are required to adhere to all policies and procedures established by the College, both for the campus network, and for other networks and systems accessed through this gateway.

3.1 Employees connect to the campus network using College-owned computers, located in offices, classrooms or labs. Special permission must be obtained to connect personally owned computers to the campus network. Those who connect personal computers must allow the College to install the same key protections used on College-owned computers, and must sign a form agreeing to abide by these *Terms and Conditions*.

3.2 Students in campus housing may connect personal computers to the campus network from their rooms, and are expected to abide by all of the policies contained in these *Terms and Conditions* in their use of the campus network and the Internet. Students may not allow others to connect to their personal computers using wired or wireless connections.

3.3 Employees or students with notebook computers will be able to connect to the campus network at locations set aside for this purpose, using either wired or wireless access as appropriate. In order to use these connections, users must have valid College accounts and be able to provide appropriate authentication.

3.4 Individuals may not connect wireless access points to the College network, in any College-owned facility.

4.0 Intended Uses of Campus Systems and Network

The campus network and systems are to be used primarily for activities related to the educational mission of the College.

Terms and Conditions

Personal use of the network is limited to transacting email and accessing Intranet or Internet Web pages. *Individuals are not allowed to operate servers of any kind on the campus network.*

By signing the form referred to in sections 2.1 and 2.2 above, you agree to abide by the policies set forth in these *Terms and Conditions*, including the following:

- agreement not to publish, on any system connected to the campus network, and not to include in any email communication, information which violates or infringes upon the rights of any other person, which is abusive, profane or sexually offensive, or which contains advertising or solicitation for goods or services;
- agreement not to transmit via the campus network copyrighted documents or media for which you do not have written authorization from the copyright owner;
- agreement not to use the campus network to conduct commercial or business activities, or to perform or solicit others to perform any activity prohibited by law.

5.0 Intended Uses of the College Internet Connection

The College recognizes the value of Internet access to its mission, as well as for personal communication. However, the College's Internet resource is limited, expensive, and shared by many users. Personal use, other than for email and Web access, is not permitted. The College reserves the right to block traffic which creates congestion but contributes no value to the College's mission.

6.0 Email

The College email system is for use by faculty, staff, and students. All messages transacted are normally retained until deleted by the recipient. Once an account has been terminated, however, no email will be retained unless required by law. Email users are assigned storage quotas and must manage their email accounts in such a way as to stay within quotas.

6.1 Email content. All users of College email are expected to abide by acceptable use policy as stated in these *Terms and Conditions*. College policy prohibits sending email containing defamatory, abusive, obscene, sexually oriented, threatening, racially offensive or illegal material. Since the College may be held responsible for inappropriate use of its email system, it may utilize monitoring software to screen email sent through the campus email system.

College employees will not normally inspect the contents of email sent to an identified addressee, or disclose such contents to anyone other than the sender or intended recipient, without consent, unless required to do so by law or by the policies of the College, or to investigate complaints regarding email alleged to contain defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

The College will cooperate fully with local, state, and federal officials in investigations related to email transmitted using College computing systems, the campus network, or the College Internet connection.

6.2 Official Communication. Official notifications are increasingly sent by email, rather than on paper. Email used for such notifications will be delivered to the recipient's College email account. Employees and students are expected to read their campus email, and must use their campus email accounts in official communication with campus offices, to ensure proper identification.

6.3 Restraint in using email. College email should not be used: (a) to create or forward "chain letters" or "pyramid schemes"; (b) to send or forward "junk mail" or "spam" to individuals not specifically requesting it; (c) to send email using forged addresses or headers; or (d) to broadcast a message to a large number of recipients.

The rule of thumb for (d) above is that a message should not be sent to more than forty recipients. This allows broadcasts to be sent to classes, clubs or committees, and other small groups. It does not allow a list of hundreds or thousands of recipients to be broken up into many small lists, to circumvent the "rule of forty."

6.4 Normal account termination. Students or employees who leave the College will have their email accounts terminated. Employee email accounts will normally be terminated on the last day of employment. Students may continue to use College email for up to 30 days after withdrawal or graduation, to permit time for making other arrangements and notifying friends and family of the new email address.

7.0 Confidentiality of User Data

7.1 User data on the campus network. The College will treat data created and/or transmitted on its network and computer systems as confidential. Confidentiality in this context does not imply complete privacy; only that access is limited to individuals authorized by the College. Whenever possible, user privacy will be respected, but this cannot be viewed as absolute. College personnel can and will access files when necessary for maintaining the campus network and computer systems. Every effort will be made to respect privacy of user files, and the contents of user files will be examined only when it is required by law or by the policies of the College.

7.2 Legal issues relating to privacy. The College is careful to abide by the requirements of the *Family Educational Rights and Privacy Act (FERPA)* and the *Gramm-Leach-Bliley Act*, both of which mandate that institutions implement safeguards for certain information pertaining to students and other customers.

7.3 Data on personal computers. User data on personal computers connected to the campus network is private, and College personnel are not authorized to obtain access to such data. System status information, which may be used to diagnose and protect against system vulnerabilities and as necessary to monitor software license compliance, will be accessed routinely by the network security service described in Section 12 below.

8.0 Internet Blocking and Proxy Services

Those who use the campus network as a gateway to the Internet have access to networks and computer systems which contain information over which the College has no control. The College reserves the right to block access to subject matter on the Internet which is in conflict with the College's *Community Covenant*.

The College's Board and Senior Administration have mandated that attempts to access sexually explicit or pornographic materials, or websites devoted to gambling, by way of the College Internet connection be blocked, logged, and reported. Students and employees who show evidence of attempted access to such materials are subject to disciplinary action.

Terms and Conditions

8.1 The Campus Proxy Server. A proxy server mediates access to Internet web pages. It use enables access to certain materials to be restricted. The College managed proxy must be used for all Internet access. Use of other proxy servers, or of the above proxy server on any port other than port 80 is prohibited, and considered a violation of the Acceptable Use Policy of these *Terms and Conditions*.

9.0 On-line Conduct

Your signature on the appropriate form, as indicated in sections 2.1 and 2.2 above, signifies that you agree not to submit, publish, or display, on any network or computing system accessed through your College account, any material which is defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal.

Transmission of any material, information or software in violation of any local, state or federal law is prohibited. Your signature on the form indicates your agreement to indemnify the College for any loss, costs or damages, including reasonable attorneys' fees, incurred by the College relating to, or arising from, any breach of this policy.

9.1 Commercial or Business Activity. Users of College computer systems or the campus network may not use these to engage in commercial or business activity.

9.2 Authorized Software. Only software for which the owner or copyright holder has given written consent for on-line distribution may be transferred to or stored on College systems, or operated on computers connected to the campus network. Software designed to interfere with others' use of computing systems or networks is prohibited. The College reserves the right to terminate accounts and/or ResNet privileges of users who violate this policy.

9.3 Copyrighted Material. Copyrighted material must not be placed on College computing systems, and the campus network may not be used to transfer such material, without written permission. Only the author(s) or those they specifically authorize may transfer copyrighted material from other media to College computing systems. Material in this category includes not only human readable documents, but also software and data files used with software designed to play musical, video, or multimedia productions. In particular, providing access to copyrighted MP3 files from media is prohibited.

9.4 Public Domain Material. Users may upload public domain programs or non-copyrighted information using the College's computing systems. Users assume all risks regarding the determination of whether such programs or other materials are in the public domain.

9.5 Inappropriate Material. Off-campus systems to which College users have access may contain material that is abusive, defamatory, inaccurate, obscene, profane, sexually oriented, threatening, racially offensive, or illegal. The College reserves the right to monitor its computer systems and campus network to ensure that such materials are not present. Students or employees who knowingly bring such materials into the College computing environment will be subject to the same disciplinary policies which apply in other campus situations. Electronic forums do not constitute a separate universe of discourse, governed by a separate ethic, but are governed by the same moral and ethical guidelines which apply to other means of discourse.

9.6 Message Boards. The College has no control over the content of messages on external message boards, but all con-

tent posted by College users to any message board must adhere to these *Terms and Conditions*. The College reserves the right to terminate accounts of users who misuse message boards.

9.7 Real-time / Interactive Communication. The use of real-time, interactive messaging systems is recognized to be of value in certain situations. The College reserves the right, however, to limit or circumscribe the use of such systems, and to terminate user accounts and/or ResNet privileges for those who misuse such services.

9.8 Security. Security on computer systems receives a high level of priority at the College. Users who identify situations that pose threats to information security are asked to notify Computing Services.

Passwords should be so chosen that they are unlikely to be guessed by others. Strong passwords usually contain mixed-case letters as well as numerals or punctuation marks. Please assist College security efforts by choosing passwords wisely, changing them periodically, and not revealing them to others.

Users should notify Computing Services if their passwords are forgotten or if there is reason to believe someone has obtained unauthorized access to their accounts.

9.9 Privacy of Information. All information on College computer systems should be considered private, unless it has been explicitly classified otherwise. Any attempt to circumvent computer or network security in order to gain access to private information is illegal, as outlined below.

10.0 Laws concerning computer usage

10.1 Computer Tampering. The Illinois Code deals with various forms of computer tampering: While some acts are classified as misdemeanors, others are considered to be felonies. See § 16D-3 of the Illinois Criminal Code.

10.2 Unlawful use of recordings. The following excerpt is from § 720 ILCS 5 / 16-8 of the Illinois Criminal Code.

Sec. 16-8. Unlawful use of unidentified sound or audio visual recordings.

(a) A person commits unlawful use of unidentified sound or audio visual recordings when he intentionally, knowingly, recklessly or negligently for profit manufactures, sells, distributes, vends, circulates, performs, leases or otherwise deals in and with unidentified sound or audio visual recordings or causes the manufacture, sale, distribution, vending, circulation, performance, lease or other dealing in and with unidentified sound or audio visual recordings.

(b) Unlawful use of unidentified sound or audio visual recordings is a Class 4 felony.

11.0 Suspension or Termination of Accounts

User accounts on College computer systems are terminated on the last day of work for employees and upon withdrawal or graduation for students. Email accounts remain active for up to 30 additional days.

The College reserves the right to suspend or terminate a user's account on College computing systems, or to suspend or terminate ResNet privileges, for breaches of policy as set forth in these *Terms and Conditions*.

Terms and Conditions

12.0 Network Security & Personal Computers

Faculty, staff, and students who wish to connect personal computers to the campus network must be able to demonstrate that their computers are protected against known vulnerabilities.

With more than 2,000 personal computers arriving on campus in a typical August, it is impossible for College technical staff to inspect, protect, and certify each computer. An automated service is necessary, and such a service has been deployed.

This service will ensure that the following protections are in place: (a) for Windows PCs, the latest service packs and critical Windows updates; (b) the College antivirus software (Sophos) is installed and operating; and (c) mechanisms to ensure that future updates will be automatic.

The goal of the service is to allow individuals to check their personal computers for vulnerabilities, and to have needed protections put in place and kept current, at any time of the year, no matter where they are.

13.0 Acceptable Use Policy for ResNet Users

The following policies extend or interpret the above Terms and Conditions with respect to ResNet usage:

13.1 ResNet services and wiring may not be modified or extended. This applies to network wiring, hardware, and in-room jacks. Use of Personal Ethernet switches or network hubs, on the campus network is expressly prohibited.

13.2 ResNet users may not allow their ResNet connection to be used by anyone outside the College community, and under no circumstances may users provide access to College systems or networks for other individuals.

13.3 ResNet users may not operate network services from their computers (BBS, Chat, DHCP, DNS, anonymous FTP, IRC, NNTP, POP2/POP3, SMTP, INS, etc.). Users who have a *bona fide* academic need to operate such services must obtain written authorization from ResNet administration prior to activating any such service.

13.4 ResNet users may not conduct port scans on the campus network, or of outside networks from the campus network, may not operate Ethernet cards in promiscuous mode, or use any IP address on the campus network other than the one(s) assigned by the College.

13.5 Commercial network resources and software that are licensed by the College for internal use only may not be used outside the College network.

13.6 Network usage that inhibits or interferes with the use of the network by others is not permitted. Applications which make heavy use of network bandwidth for extended periods of time, and applications designed to send repeated email messages or mass email messages ("email bombs" or "bulk emailers") are not permitted.

13.7 To guarantee that network resources are available to all users, pop mail clients (Eudora, Netscape Messenger, Outlook, Outlook Express, etc.), if set to retrieve mail automatically, must do so no more frequently than every thirty (30) minutes. However, users may manually retrieve mail as frequently as they wish.

13.8 ResNet may only be used for legal purposes and to access only systems, software and data to which the user has authorized access. Providing access to copyrighted software or

other material (including MP3 or similar files from copyrighted media) on the network is prohibited.

13.9 Respecting the rights of other users, including their rights as set forth in other College policies for students, faculty, and staff, is required at all times.

13.10 Users are required to know and follow the specific policies and usage procedures established for any systems and networks to which they have authorized access.

13.11 ResNet is provided for use within the context of the academic mission of the College. It may not be used for commercial purposes or for advertising. Users may not provide open access from their computers to anything protected by copyright (including MP3 files from copyrighted media), or of a sexually explicit or pornographic nature, or which violates College policy or Residence Life community standards.

13.12 Forgery or other misrepresentation of identity via electronic or other form of communication is a violation of the Community Covenant and will be subject to disciplinary action. Prosecution under State and Federal laws may also apply. This includes the use of a network (IP) address not specifically assigned to the individual, or use of a forged or false identity in sending email.

13.13 The College may refuse network access to anyone who violates its policies or abuses the rights of others. If it is suspected that a ResNet connection has been used to violate policy, that connection may be suspended without prior notice, pending investigation and resolution of the issue. The College reserves the right to scan any part of its network, including ResNet, for security problems, and to monitor traffic and usage patterns on its network.

13.14 The College retains the right to block or to disable network applications which use excessive network bandwidth or which facilitate illegal activity.

14.0 Other provisions

The *Terms and Conditions* shall be interpreted, construed and enforced in all respects in accordance with the laws of the State of Illinois. Each user irrevocably consents to the jurisdiction of the courts of the State of Illinois and the federal courts situated in the State of Illinois, in connection with any action to enforce the provisions of the *Terms and Conditions*, to recover damages or other relief for breach or default under the *Terms and Conditions*, or otherwise arising under or by reason of the *Terms and Conditions*. ♦