Reed College Computer User Agreement

Approved by the Computing Policy Committee 9/16/2005; revised 11/21/2008, revised 2/3/2011.

Reed College computing resources are provided for use by all Reed students, faculty and staff. Alumni and other individuals may use computer facilities by special permission, as guests of the College. All eligible individuals who wish to use the computing resources are required to read and accept this agreement and are expected to follow the guidelines for acceptable computer use described below.

Acceptable Uses

The use of the computer facilities is granted to the undersigned only. The undersigned shall not allow another person to use his or her username and password.

Reed's computing resources are provided primarily for academic purposes, including education, research, communication, and college administration.

Prohibited Uses

It is prohibited to use Reed's computing resources in ways that:

- infringe on another individual's right to privacy or otherwise adversely affect members of the user community;
- are inconsistent with the academic mission and not-for-profit status of the College;
- violate usage restrictions required by Reed's software, hardware, ISP, or other technology licenses;
- violate College policies or local, state, or federal statutes.

Some examples of prohibited uses are:

- unauthorized access to someone else's account, use of someone else's username and password, or unauthorized access of remote computers via Reed's network facilities;
- unauthorized reading, copying, deleting, or modification of someone else's electronic materials including email;
- intentional damage to hardware, software, network equipment, security devices, or other technology resources;
- intentional creation or distribution of viruses, worms or other forms of electronic malware;
- abuse of printing privileges, such as printing under a false username;
- sending obscene, abusive, harassing, or threatening messages;
- excessive non-academic use of network bandwidth or CPU cycles;
- unauthorized use, duplication, or sharing, of copyrighted materials, such as music, images, text, multimedia, commercial software, etc.;
- profit-making activities, such as development and sale of software or digital materials, work undertaken to support a for-profit company, or contract work unrelated to Reed's academic mission;

- not-for-profit activities unrelated to Reed's academic mission on behalf of an external organization or institution unless previously approved in writing by the president of Reed College.

Confidential Data

Reed College faculty, staff, and student employees have varying access to electronic information that is sensitive and confidential[1]. Reed College considers the protection of such information and its electronic infrastructure from unauthorized use to be a key responsibility of all faculty, staff, and student employees. Failure to act in accordance with College guidelines may result in disciplinary and/or legal action.

Confidential information must be stewarded in an ethical, professional, and legal manner at all times. All institutional data, whether maintained in a central database, on a local workstation or elsewhere, remain the property of the College and are governed by this statement.

By law, certain institutional data may not be released without proper authorization. You must adhere to all applicable federal and state laws concerning storage, retention, use, release, and destruction of data. Users are encouraged to seek guidance from an appropriate supervisor, senior officer, or the chief technology officer if it is unclear whether or not specific information is confidential.

Confidential data shall be used only as required in the performance of College duties. You may not inspect, copy, alter, delete, share, grant access to, or in any other manner use such information, except as required in the performance of your job duties.

You are responsible for the security, privacy, and control of data in your care, access privileges entrusted to you, and your username/password. If you have reason to believe that your username/password is known by or has been used by another person, you should immediately notify an appropriate supervisor, senior officer, or the chief technology officer.

You must take every reasonable precaution to prevent unauthorized access to confidential data. Such data shall not be presented or shared inside or outside the College without prior approval from the appropriate supervisor or senior officer of the College. Confidential data should never be left on any computer to which access is not controlled.

When using the institution's electronic information systems, you should exercise care to protect data from unauthorized use, disclosure, alteration, or destruction. You must understand the definition of confidential information in the context of your job responsibilities and take steps to ensure that your co-workers, staff, and student employees understand existing statutes and policies (such as FERPA, HIPAA, Donor Bill of Rights, Digital Millennium Copyright Act, etc., and College departmental guidelines that may supplement this agreement). Before granting access to confidential information you should be satisfied that a "need to know" is clearly demonstrated. You should seek guidance from an

[1] http://web.reed.edu/cis/help/id-confidential.html

appropriate supervisor, senior officer, or the chief technology officer when the appropriate use of, or the granting of access to, such information is unclear.

It is a violation of College policy, and may be a crime, for individuals to attempt to gain access to College electronic data that they do not need in the performance of their job or to which they are not authorized to have access.

Confidential or otherwise sensitive College information **must not be stored, shared, or otherwise processed** by a cloud computing service[2] unless the service enters into a legally binding agreement with Reed to protect and manage the data according to standards and procedures acceptable to the College.

Computing and Information Services (CIS) shall review requests for access to central data systems and serve as the initial point of conflict resolution in instances where requests for such access conflict with this statement.

Appropriate College procedures shall be followed in reporting any breach of security or compromise of safeguards.

Illegal Copying of Software and Other Copyrighted Materials

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of authors, artists, and publishers in all media including text, music, images, software and other domains. It encompasses respect for the right to acknowledgment and the right to determine the form, manner, and terms of publication and distribution of one's work. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical.

Copyright infringement and unauthorized access to digital materials may be grounds for legal action. Use of illegally copied software or other materials undermines Reed's ability to negotiate favorable software agreements and may result in legal action against the user as well as the College.

Reed prohibits the illegal use of copyrighted materials. Under the terms of the Digital Millennium Copyright Act (DMCA), the College is committed to respond to lawful requests for information. Reed will not protect or defend a user against criminal investigations or lawsuits resulting from intentional copyright infringement.

Fees

In general, the College does not charge students, faculty, or staff a fee for the use of computing or network resources. However, fees are charged in specific instances including:

Printing : There is a per-page charge to students for printing to networked printers in the IRCs, Library, and residence halls. Students are billed through the Business Office. Information about current rates and charges can be obtained from Computer User Services or found on the web at http://web.reed.edu/cis/help/print/

[2] http://web.reed.edu/cis/policies/cloud-computing.html

Stolen computers : Under certain circumstances, faculty and staff may be charged a fee in the event that College-provided computing equipment in their care is lost, stolen, or damaged beyond repair. A policy describing the details of potential employee liability are provided on the web at: http://web.reed.edu/cis/policies/theft_loss.html

Storage and Transmission of Electronic Materials

The College respects individuals' right to privacy and takes steps to prevent unauthorized access to electronic materials stored or transmitted via College computing or network equipment. However, the College reserves the right to examine such materials at its sole discretion in certain cases, for example, when it believes that there is a potential violation of a law or of College policy.

The College may use email to communicate with members of the college community. Students and employees are generally expected to check their email regularly, as they would their paper mail.

Users are reminded that the storage and transmission of electronic materials, including email, can be disrupted by hardware and software failure as well as by hacking or other unauthorized access. Users are cautioned about storing or transmitting material which they view as sensitive or confidential. It is the user's responsibility to back up their material except for instances where the College specifically commits to provide backups.

Computer User Services is NOT responsible for personal files stored on hard drives in student Information Resource Centers (IRCs). Users are responsible for saving personal files to their own disk(s). IRC hard disks are cleaned on a regular basis and extraneous files are deleted. Centralized disk storage is available to all students, faculty, and staff and may be requested by contacting Computer User Services (for staff: Administrative Computing Services).

Requests for Access to Email and other Files by Third Parties

From time to time, CIS may receive internal or external requests for access to employee's or student's electronic mail and other files, including system, network, and user audit logs. In cases where a request is made as part of an eDiscovery process, CIS response shall be governed by the guidelines set forth in the *Reed College eDiscovery Guidelines* available on the web at: http://web.reed.edu/cis/policies/index.html

Request that do not fall under eDiscovery shall be governed by the following guidelines for CIS staff:

- The chief technology officer shall be notified immediately of the request
- CIS shall obtain guidance from legal counsel and/or a senior officer of the college regarding the legitimacy of providing access to the requested material
    - if a request involves file of a staff member, the VP/Treasurer and/or the Director of Human Resources shall be notified
    - if a request involves file of a student, the VP of Student Services shall be notified

- CIS shall obtain guidance from legal counsel and/or a senior officer of the college regarding the need for someone to review the material before access is granted and, if a review is required, shall be notified of the individual(s) who will conduct the review

- In the event of a review, CIS will contact the reviewer(s) to determine the technical format for delivering the electronic materials to expedite the review while minimizing or eliminating any impact upon the content (for example: emails may be downloaded in chronological sequence and formatted as a .pdf, .txt or other type of searchable file without altering heading or body information)

- Upon completion of a review, the reviewer(s) will notify CIS in writing as to whether or not the request for access should be granted and, if so, the manner in which the electronic materials should be delivered to the individual(s) who initiated the request.

At no time shall CIS staff members examine the contents of email or other user files in response to an access request by a third party unless so required in order to fulfill their responsibilities or directed to do so by the chief technology officer, the director of community safety, a senior officer of the college, or college legal counsel.

Failure to Comply

The College will suspend or revoke the computing privileges of anyone who violates this agreement or fails to pay a required fee. The terms and conditions of usage are subject to change as computing resources and user demands vary. This policy is reviewed on an annual basis by the Computing Policy Committee. The Reed community will be notified if the agreement is changed. The current version will be available at the CIS website at:

http://web.reed.edu/cis/policies/user_agreement.html

Ongoing use of Reed's computing facilities and services implies your acceptance of the most current version of this agreement. Users who decline to accept the current version will be prohibited from using Reed's computing facilities and services.

If a computer user fails to comply with these terms and conditions, CIS will follow the "Procedures for Handling Violations of the User Agreement," located at
http://web.reed.edu/cis/policies/violations_procedures.html

Other policies related to the use of Reed's computing resources may be found at:

http://web.reed.edu/cis/policies/index.html

Access to the Internet via Reed's Internet Service Provider (ISP), must conform to Time Warner Telecommunications' Acceptable Use Policy available on the web at:

http://info.twtelecom.net/info.php?id=2

By accepting this agreement, the user acknowledges that he or she has read, understands, and agrees to comply with its provisions and other policies governing the use of Reed College computing and networking facilities. This agreement covers all computing equipment owned by the College as well as remote computing resources accessible through the College's communication facilities.

For further information, contact the Reed College Office of Computer User Services at 503-777-7525 or via electronic mail at cus@reed.edu

Acceptance Declaration

I have read and understood the provisions and legal restrictions described above and other policies governing the use of Reed College computing resources referenced in this agreement. I understand that the agreement covers all computing resources owned by the College as well as remote computing resources accessible through the College's electronic communication facilities.

I further understand that use of Reed's computing resources is a privilege, not a right, and that if the terms of this agreement are violated the College may issue a warning, deny access to computing resources, refer for prosecution, or administer other penalties, depending upon the nature of the infraction.

Complete and sign the form on the following page.

Full Name: Date:

_____

Signature

Staff/Student Employee Information (please write clearly)

Name: _____

Reed ID Number: _____ Location: _____Dept:_____

Phone: _____ ❑ Student ❑ Staff Title: _____

Supervisor's Signature:_____

Please check off the accounts/services that are needed for this community member:

❑ Email ❑ MeetingMaker ❑ Brio
❑ Portfolio (please describe type of access or list staff member whose Portfolio privileges should be copied_____)
❑ Banner Forms (please describe type of access or list staff member whose Banner privileges should be copied_____)
❑ College Relations Datamart (please describe type of access or list staff member whose Banner privileges should be copied_____)
❑ access to unix host alice ❑ access to unix host lory
❑ Advancement Self-Service (aka Web for Development Officers; level of access?_____; birthdate?_____)
❑ EMS (level of access?_____)

Additional One-Card access ❑ Eliot Hall after hours ❑ Library Staff ❑ ETC 3rd Floor ❑ CIS staff ❑ FML (faculty multimedia lab) ❑ CSO ❑ Facilities/Custodial

❑ Other _____

---

office use only

Kerberos UID#: _____Unix host login: _____

Unix ❑ Banner Forms ❑ AdminNT ❑ EMS ❑ Portfolio ❑ Meeting Maker ❑ Datamart ❑ Brio

❑ Advancement S-S ❑ Date: _____ ACS Initial: _____