

Acceptable Use of Information Technology Resources at Lake Forest College

Information technology plays an integral part in the fulfillment of Lake Forest College's core academic mission. Users of LFC's IT resources have a responsibility not to abuse those resources and to respect the rights of the members of the community as well as the College itself. This appropriate use policy document provides guidelines for the appropriate use of LFC's IT resources as well as for the College's access to information about and oversight of these resources.

For the purposes of this policy, technology resources are defined as all computer-related equipment, computer systems, software/ network applications, interconnecting networks, facsimile machines, voicemail and other telecommunications facilities, as well as all information contained therein (collectively, "electronic resources") owned or managed by Lake Forest College.

The use of Lake Forest College's technology resources is a privilege, not a right, which may be revoked at any time for abuse and/or misuse. Lake Forest College reserves the right to limit access to its electronic resources when applicable College policies, state and/or federal laws or contractual obligations are violated. The College does not, as a rule, monitor the content of materials transported over the College's network resources or posted on College-owned computers and networks, but reserves the right to do so. Although the College does not typically block access to online content it reserves the right to do so in cases where online content or activity diminishes the capacity of our network, or where there is a threat to the Lake Forest College or its mission. Lake Forest College provides reasonable security against intrusion and damage to files stored on the central computing facilities, but does not guarantee that its computer systems are secure. Lake Forest College may not be held accountable for unauthorized access by other users, nor can the College guarantee protection against media failure, certain computer-borne viruses, fire, floods, or other natural or man-made disasters.

I. Scope

This policy applies to all users of technology resources, including but not limited to LFC students, faculty, staff, alumni, and others who have been granted permission by the Office of the Library and Information Technology to use these resources. It applies to the use of all technology resources whether these resources are accessed from on campus or from off campus locations. These resources include systems, networks, and facilities administered by the Office of the Library and Information Technology (LIT).

II. Appropriate Use of IT Resources

All users of Lake Forest College electronic resources are expected to utilize such resources in a responsible, ethical and legal manner consistent with Lake Forest College

policies. Although this Policy sets forth the general parameters of appropriate use of IT systems, students, faculty, staff, and alumni should consult their respective governing policy manuals for more detailed statements on permitted use and the extent of use that the College considers appropriate in light of their varying roles within the community.

- A. *Appropriate Use.* LIT systems may be used only for their authorized purposes -- that is, to support the research, education, administrative, and other functions of Lake Forest College. The particular purposes of any LIT system as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the user.
- B. *Proper Authorization.* Users are entitled to access only those elements of LIT systems that are consistent with their authorization.
- C. *Specific Proscriptions on Use.* The following categories of use are inappropriate and prohibited:
 1. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.
 2. Use that is inconsistent with Lake Forest College's non-profit status. The College is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT systems for non-LFC purposes is generally prohibited, except if *specifically* authorized and permitted under College conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the College's educational, administrative, research, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.
 3. Use of IT systems in a way that suggests College endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes College involvement, except for authorized lobbying through or in consultation with the administration of the College.
 4. Harassing or threatening use. This category includes, for example, display of illegal or offensive, sexual material in the workplace and repeated unwelcome contacts with another user.

5. Use damaging the integrity of College or other IT systems. This category includes, but is not limited to, the following six activities:

III. Attempts to defeat system security.

Users must not defeat or attempt to defeat any LIT system's security -- for example, by "cracking" or guessing and applying the identification or password of another user, or compromising room locks or alarm systems. (This provision, however, does not prohibit LIT staff from using security scan programs within the scope of their authority).

A. *Unauthorized access or use.* The College recognizes the importance of preserving the privacy of users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to LIT systems, nor permitting or assisting any others in doing the same. For example, a non-LFC organization or individual may not use non-public LIT systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-LFC organizations or individuals across the LFC network without specific authorization. Similarly, users are prohibited from accessing or attempting to access data on LIT systems that they are not authorized to access. Furthermore, users must not make or attempt to make any deliberate, unauthorized changes to data on an LIT system. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network "sniffers," or otherwise tapping phone or network lines.

B. *Disguised use.* Users must not conceal their identity when using LIT systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

C. *Distributing computer viruses.* Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

D. *Modification or removal of data or equipment.* Without specific authorization, Users may not remove or modify any College-owned or administered equipment or data from LIT systems.

E. *Use of unauthorized devices.* Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, printer, or video system) to LIT systems.

F. *Use in violation of law.* Illegal use of IT systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

G. *Copyright.* With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not mean that the use is permitted without authorization.

H. *Use in violation of College contracts.* All use of IT systems must be consistent with the College's contractual obligations, including limitations defined in software and other licensing agreements.

I. *Use in violation of College policy.* Use of IT systems which results in the violation of other College policies is also a violation of this policy. Relevant College policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment.

J. *Use in violation of external data network policies.* Users must observe all applicable policies of external data networks when using such networks.

K. *Personal Account Responsibility.* Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any user changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages.

L. *Responsibility for Content.* Official College information may be published in a variety of electronic forms. Deans, directors, and department chairs under whose auspices the information is published are considered the certifying authority for such information and are responsible for the content of the published document. Users also are able to publish information on IT Systems or over LFC's networks. Neither the College nor the appropriate LIT staff can screen such privately published material nor can they ensure its accuracy or assume any responsibility for its content. The College will treat any electronic publication provided on or over IT systems that lacks a certifying authority as the private speech of an individual user.

IV. Privacy and Conditions of College Access

The College places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the College may determine that certain broad concerns outweigh the value of a user's expectation of privacy and warrant College access to relevant

IT systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

A. *Conditions.* In accordance with state and federal law, the College may access all aspects of IT Systems, without the consent of the user, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT systems; or
2. When required by federal, state, or local law or administrative rules; or
3. When there are reasonable grounds to believe that a violation of law or a significant breach of College policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
4. When such access to IT systems is required to carry out essential business functions of the College; or
5. When required to preserve public health and safety.

B. *Process.* Consistent with the privacy interests of users, College access without the consent of the user will occur only with the approval of the Dean of the Faculty (for faculty users), the Vice President for Business (for staff users), the Dean of Students (for students), or their respective appointees, except when an emergency entry is urgently necessary to preserve the integrity of facilities or to preserve public health and safety. The College, through the Director of LIT, will log all instances of access without consent. LIT staff will also log any emergency entry within their control for subsequent review by the Dean of the Faculty, the Vice President for Business, or the Dean of Students.

C. *User access deactivations.* In addition to accessing the IT systems, the College may deactivate a user's IT privileges, whether or not the user is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data. LIT staff will attempt to notify the user of any such action.

D. *Use of security scanning systems.* By connecting privately owned personal computers or other IT resources to the College's network, users consent to College use of scanning programs for security purposes on those resources while attached to the network.

V. Enforcement Procedures

A. *Complaints of Alleged Violations.* An individual who believes that he or she has been harmed by an alleged violation of this policy may file a complaint in accordance with established College grievance procedures (including, where relevant, those

procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Director of LIT, who must investigate the allegation and (if appropriate) refer the matter to College disciplinary and/or law enforcement authorities.

B. *Reporting Observed Violations.* If an individual has observed or otherwise is aware of a violation of this policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Director of LIT, who must investigate the allegation and (if appropriate) refer the matter to College disciplinary and/or law enforcement authorities.

C. *Disciplinary Procedures.* Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the Faculty Handbook, the Administrative Handbook, the Non-Academic, Non-Exempt Staff Handbook, the Student Handbook, and other applicable materials.

LIT staff may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, LIT staff are authorized to investigate alleged violations.

D. *Penalties.* Individuals found to have violated this policy may be subject to penalties provided for in other College policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The applicable disciplinary authority in consultation with the Director of LIT shall determine the appropriate penalties.

E. *Legal liability for unlawful use.* In addition to College discipline, users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT system.

F. *Appeals.* Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures. Appeals should be directed to the appropriate Dean or Vice President.

VI. Policy Development

This Policy may be periodically reviewed and modified by the members of the LIT staff, the Dean of the Faculty, the Dean of of Students, the Vice President for Business, and the LIT Advisory Committee, who may consult with appropriate College committees, faculty, students, and staff.