1.3 A

Information technology ("IT"), the vast and growing array of computing and electronic data communications facilities and services, is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information technology plays an integral part in the ful°llment of Saint Louis University's research, education, clinical, administrative, and other roles. Users of Saint Louis University'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 University itself. This Saint Louis University IT Appropriate Use Policy (the "Policy" or "AUP") provides guidelines for the appropriate use of Saint Louis University's IT resources, as well as for the University's access to information about and oversight of these resources.

Most IT use parallels familiar activity in other media and formats, making existing University policies important in determining what use is appropriate. Using electronic mail ("e-mail") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. University policies that already govern freedom of expression and related matters in the context of standard written expression govern electronic expression as well. This Policy addresses circumstances that are particular to the IT arena and shall augment but not supersede other relevant University policies.

Users should familiarize themselves with any supplementary or speci°cally tailored policies that also govern use of information technology systems. The Division of Information Technology Services ("ITS") and other divisions that manage IT Systems may develop and promulgate system-speci°c policies in association with appropriate governing bodies. External service-providing organizations may also have speci°c usage policies. Such policies must be consistent with this Policy and provided to the V

. D

These include but are not limited to the computers, terminals, printers, networks, modem banks, online and o [1]

- To ensure that IT Systems are used for their intended purposes; and

well as the nature and scope of personal use may vary according to the duties and responsibilities of the User or the type of personal use.

B. Users are entitled to access, modify, or delete only those elements of IT Systems that are consistent with their authorization. Any attempt to accumulate unauthorized information or misuse of information appropriately obtained is strictly prohibited.

C. The following categories of use are inappropriate and prohibited:

1. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including, without limitation, "resource hogging," misuse of mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading e-mail or postings widely and without good purpose), or "bombing" (»ooding an individual, group or system with numerous or large e-mail messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network tra ¸ c or computing load is also prohibited.

2. The University is a non-pro°t, tax-exempt organization, and as such, is subject to speci°c 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-Saint Louis University purposes is generally prohibited, unless speci°cally authorized and permitted under other University policies. Prohibited commercial use does not include communications and exchange of data that furthers the University's educational, administrative, research, clinical, and other roles, regardless of whether it has an incidental °nancial or other bene°t to an external organization.

   Use of IT Systems in a way that suggests University endorsement of any political candidate or political initiative is also prohibited. Users must refrain

from using IT Systems for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation with an authorized University o ¸ cial.

3. Use in violation of other University policies or use that is inconsistent with the University's Catholic Jesuit mission and ideals also violates this policy. Such other University policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, conduct codes of the various schools and colleges, and speci°c University departmental and work-unit policies and guidelines regarding incidental personal use of IT Systems.

4. This category includes, but is not limited to, the following six activities:

   a. Users must not defeat or attempt to defeat any IT System's security - for example, by "cracking" or guessing and applying, possessing, and/or using the identi°cation or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit ITS or Systems Administrators from using security scan or other similar programs within the scope of their Systems Authority.)

   b. The University recognizes the importance of preserving the privacy of Users and data stored in IT systems. Accordingly, Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-Saint Louis University organization or individual may not use non-public IT Systems without speci°c authorization.

      Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-Saint Louis University organizations or individuals across the Saint Louis University network without speci°c authorization. Similarly, Users are

prohibited from accessing or attempting to access data on IT 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 IT System.

Users must not intercept or attempt to intercept or access data communications not intended for that User, such as promiscuous network monitoring, running network sni · ers, or otherwise tapping phone or network lines.

ITS sta · is prohibited from engaging in any intrusive investigations not authorized in accordance with ITS Policy on intrusive investigations.

c

- infringing copyrights; and
- making bomb or other threats.

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 automatically mean that the use is permitted without authorization.

6. All use of IT Systems must be consistent with the University's contractual obligations, including limitations de°ned in software and other licensing agreements.
7. Users must observe all applicable policies of external data networks when using such networks.
8. Users of IT Systems may exercise rights of free inquiry and expression consistent with provisions contained in the Student Handbook, the Faculty Manual, or the Sta · Handbook, as may be appropriate, and the principles of academic freedom at Saint Louis University.
9. Users must maintain the security of their own IT Systems accounts and passwords, and they are responsible for any breaches in the security of those accounts or passwords which are caused by their own negligence, recklessness or unlawful actions. Any User changes of password must follow prescribed guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users have the responsibility to control the activities which they permit others to carry out under

storage or in transit. Any encryption of University-related data performed on an IT System must use software and protocols endorsed by ITS and such encryption must permit properly designated University o ¸ cials, upon the direction of the Vice President/Chief Information O ¸ cer, to decrypt the information. Upon request of the Vice President/Chief Information O ¸ cer, a User shall decrypt any encrypted information, including without limitation, data, documents and messages.

11. O ¸ cial University information may be published in

The University places a value on privacy and recognizes its importance in an academic setting. There are circumstances nonetheless in which, following prescribed processes and procedural safeguards established to ensure access is gained only when and to the extent appropriate, the University may determine that certain University concerns outweigh the value of a User's privacy and warrant University access to relevant IT Systems without the consent or knowledge of the User. Accordingly, in the circumstances described below, use of University IT Systems should not be considered to be private.

A. In accordance with state and federal law and published University policies, the University may access any aspects of IT Systems, without the consent or knowledge 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;
2. When required by federal, state or local law;
3. When there are reasonable grounds to believe that a violation of law or a breach of any of the proscriptions of Section V.C., of this Appropriate Use Policy may have taken place and access and inspection or monitoring may produce evidence related to the suspected misconduct;
4. When such access to IT Systems is required to carry out essential business functions of the University; or
5. When required to preserve public or campus health, safety, or order.

B. Consistent with the privacy interests of Users, University access without the consent or knowledge of the User will occur only with the approval of the President, Provost, or their designee or the Vice President/Chief Information O ¸ cer, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public or campus health, safety, or order or when such access is necessary for IT Systems maintenance when such is conducted in accordance with established procedures and in accordance with provisions of Section VI.A.

B.

conduct. Violators may also incur other IT-speci