Information Technology Acceptable Use Policy

Overview

The information technology resources of Providence College are owned and maintained by Providence College. Use of this technology is a privilege, not a right, and users have certain responsibilities. Use of the College's information technology resources should be in conformity with the mission, goals, and values of Providence College. Use of the College's technology, therefore, should be supportive of its educational and research roles, as well as its values and behavioral standards.

Acceptable use of the College's information technology resources is consistent with the principle of academic freedom. As is the case with the use of all other resources and activities provided or sponsored by the College, however, use of the College's information technology resources is contingent upon adherence to ethical and legal behavioral expectations, and compliance with policies and procedures outlined in the College's *Handbooks* (Student, Faculty, Staff). Legitimate use of a computer, computer system or network, does not extend to whatever is technically possible. Users should note that college information technology resources may be accessed by minors.

Effective security is a community-wide effort involving the support and participation of all Providence College students, employees and affiliates who deal with information and/or information systems. Members of the Providence College community are expected to become familiar with this Acceptable Use Policy, to act with careful consideration of its requirements, and to seek assistance whenever necessary.

Purpose

The purpose of this policy is to outline the acceptable use of computer systems, networks, and other information technology resources at Providence College. These rules are in place to protect students, faculty, staff and the College. Inappropriate use exposes Providence College to a number of risks, including but not limited to virus attacks, compromise of network systems and services, and legal liability.

Scope

This policy applies to students, faculty, staff and agents of Providence College, including all personnel affiliated with third parties.

Guidelines for General Use

1. Information technology resources are provided to support the academic and administrative goals of Providence College. These resources are limited and should be used with consideration for the rights and needs of others.

2. Information distributed through Providence College’s information technology resources may be considered a form of publication. Users of these resources should employ appropriate language and communication methods.
3. Unless postings from a Providence College email address to public forums are clearly in the course of the College’s academic or administrative duties, they should contain a disclaimer stating that the opinions expressed are strictly those of the poster and not necessarily those of Providence College.
4. Automated forwarding of Providence College email is not supported or allowed.

Unacceptable Use

The activities listed below are prohibited. The list of prohibited activities is not all inclusive; rather, it includes examples of what the College considers to be clearly inappropriate behavior and unacceptable uses of its information technology resources.

1. Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Providence College or the owner of the computer.
2. Unauthorized use of copyrighted material including, but not limited to, photographic images or copyrighted music, and the installation of any copyrighted software for which Providence College or the end user does not have an active license.
3. Introduction of malicious programs into the network or servers.
4. Unauthorized disclosure or use of an account password, or an attempt to access, or actual access to, an information technology resource by providing false or misleading information.
5. Use of an information technology resource to create, post, transmit or receive material or messages that violate the College’s harassment policy and/or applicable law.
6. Use of an information technology resource to view, create, post, transmit or receive material deemed by the College obscene, unless such activity is appropriate for academic or work purposes.
7. Use of an information technology resource to threaten or vilify others.
8. Use of an information technology resource for commercial gain, product advertisement, or political activities unless expressly authorized by a senior member of the College’s administration.
9. Use of an information technology resource to make fraudulent offers of products, items, or services.
10. Deliberate disruption of the College’s computer systems, networks or other information technology resources.
11. Port scanning or security scanning without prior approval by Information Technology.
12. Circumvention of user authentication or security of any host, network or account.

13. Use of an information technology resource to access or transmit the files or communications of other students, faculty or staff without authorization, or to provide information about, or lists of, students, faculty or staff to persons, groups, or organizations outside the College without authorization.
14. Use of an information technology resource to engage in any activity that is illegal under local, state, federal, or international law.
15. Use of an information technology resource to send unsolicited email messages such as "junk mail" or other advertising material to individuals who did not specifically request such material.
16. Use of an information technology resource such as email, telephone, paging, text messaging, instant messaging, or any other new electronic technologies that may emerge, to engage in any form of harassment in violation of College policy and/or applicable law.
17. Unauthorized use of email header information, or forgery of email header information.
18. Use of an information technology resource to create or forward "chain letters" or other "pyramid" schemes of any type.

Security and Safeguarding of Information Technology Resources

1. Authorized users are responsible for the security of their passwords and accounts. The use of individual accounts should not be shared with another user. Passwords should be changed on a routine basis.
2. All computers that are connected to the Providence College network must be running virus-scanning software with a current virus database.
3. All computers that are connected to the Providence College network must be up to date with all operating system updates and patches.
4. E-mail attachments received from unknown senders may contain viruses, e-mail bombs, or Trojan horse codes; therefore, they should not be opened and they should be deleted.

Confidentiality

Records maintained by the College, including those in computerized form, are vital College assets. Information contained in those records, including but not limited to academic, financial, and personnel records, are considered confidential and private. Every reasonable effort will be made to limit access to such records to authorized individuals only. The College may be compelled to release confidential records to comply with legal obligations.

Users of the College’s information technology resources who are authorized to access confidential records must respect the privacy rights of others and use such data only for legitimate academic or administrative purposes. Users with access to confidential data must protect the accuracy, integrity, and confidentiality of that data by taking all necessary precautions and following established safeguarding procedures.

Privacy Regarding the Use of Information Technology Resources

The College employs various measures to protect the security of its information technology resources and its users' accounts. Users should be aware, however, that the College cannot guarantee such security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

Users should be aware that their use of the College's information technology resources is not completely private. While the College does not routinely monitor individual use of its information technology resources, the normal operation and maintenance of the College's information technology resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. In addition, the College's network administrators and others may view data downloaded from the Internet by users.

The College also may specifically monitor the activity and accounts of individual users of the college information technology resources, including but not limited to, individual login sessions and communications, without notice, when:

1. the user has voluntarily made them accessible to the public, by, for example, posting to SAKAI or a Web page;
2. it reasonably appears necessary to do so to protect the integrity, security, or functionality of College or other information technology resources, or to protect the College from liability or other potentially adverse consequences;
3. there is reasonable cause to believe that the user has violated, or is violating, the Information Technology Acceptable Use Policy and/or policies prohibiting harassment and violent behaviors;
4. an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns;
5. it is otherwise required or permitted by law.

Any such monitoring of communications, other than what is made accessible by the user, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the appropriate Vice President or the Assistant Vice President for Information Technology, in consultation with the General Counsel, or their designees.

The College, at its discretion, may disclose the results of any such general or specific monitoring, including the contents and records of individual communications, to appropriate College personnel and law enforcement agencies, and may use those results in appropriate College disciplinary proceedings. Communications made by means of College information technology resources are also generally subject to court orders, valid subpoenas, or other legally enforceable discovery requests to the same extent as they would be if made on paper.

Wireless Networking

Individual or departmental deployment of wireless networks is not allowed. Providence College provides supported wireless “hot spots” on its campus. These “hot spots” are available only to members of the Providence College community. Any unauthorized wireless access point found connected to the campus network will be considered a security risk and disabled.

Procedure for Reporting an Alleged Misuse of the Computer Systems

Suspected violations of this Acceptable Use Policy should be reported in a timely fashion, in writing, to the Information Security Officer. Email may be sent to infosec@providence.edu. In order to help ensure the fairness of any subsequent investigation, the individual filing the report should not discuss with or provide copies of the report to other persons. Nothing in this reporting procedure shall be interpreted to prohibit an individual from pursuing such other administrative or legal rights as he or she may have and deem necessary.

Enforcement

When presented with evidence of a violation of College policies, or state or federal laws, or when it is necessary to do so to protect the College against potential legal liability, the College may suspend, block, or restrict the use of its information technology resources. Violators also may be subject to other penalties and disciplinary action, including possible suspension, dismissal, or termination.

Latest Policy Revision Date: October, 2012