

# Princeton University Information Technology Policy

## 2011-2012 Edition

---

The Princeton University Information Technology Policy sets forth the central policies governing all uses of the University's information technology resources whether administered by the Office of Information Technology or individual departments. As stated in *Rights, Rules, and Responsibilities*, members of the University community are expected to be familiar with and adhere to these policies.

### ***Introduction to Princeton University IT Policy***

#### **IT policies**

The Princeton University Information Technology Policy (the "Policy") is the central information technology policy document for Princeton University. Departments and offices of the University that create specialized computing or network policies for their constituencies must work with the University's Office of Information Technology (OIT) before doing so in order to ensure that such specialized policies are consistent with, and not in conflict with, the Policy. Once approved, such specialized policies will be cross-referenced in future editions of the Policy.

In addition, Princeton's technological and information resources and the access provided by the University to global networks and networked resources are therefore governed by the general policies and rules set forth in Princeton University *Rights, Rules, Responsibilities*. For example, policies and rules set forth in *RRR* that apply to property, privacy, civility and publication in the physical sense also apply to those areas when they involve computers or mobile devices; when they entail use of, or publication via, the World Wide Web or Internet, message boards, wikis and other "social networks" or "chat rooms;" when they consist of e-mail, texting, tweeting or instant messaging; when they involve participation in virtual reality environments, or whether the technology involved is something like the campus voice-mail, or locally-produced and broadcast video.

#### **Reasons**

Some rules for appropriate use of the University's information resources and technologies derive from legal considerations. For example, the University must ensure that its non-profit status with the Internal Revenue Service is not compromised by inappropriate political campaign or commercial activity. The University must also address actions that may violate its agreements with outside vendors.

The University is a "carrier" of information via electronic channels rather than a "publisher" and hence, except with regard to official University publications, not expected to be aware of, or responsible for, material or communications that individuals may post, send, or publish via the World Wide Web, Internet discussion groups, or social networks; make available via any file-

sharing method, or send via e-mail, tweeting or instant messaging; or any actions taken by individuals' avatars within on-line virtual reality environments. However, under certain circumstances, the University may be required to respond to complaints regarding the nature or substance of such materials or communications.

### **Changes**

The examples presented in this publication focus on matters related to the technologies, but derive their broader meaning and significance from the basic rights, rules and responsibilities that apply to all aspects of the University community. The examples are illustrative, not exhaustive. If something is not specified in the Policy as inappropriate, it still may transgress University regulations if it violates the principles set forth in *Rights, Rules, Responsibilities*. It is important to use common sense and critical thinking in evaluating new situations.

Because the technology changes so rapidly, and the human imagination is boundless in exploring what technology can do, this Policy must and will continue to evolve. In addition, the University's Rights and Rules Committee is charged with the task of revising the code in *Rights, Rules, Responsibilities*, and any changes approved by the Council of the Princeton University Community (CPUC) could affect the language of this Policy.

### ***Who must comply? What penalties pertain?***

#### **Compliance**

University policies apply to university-owned devices and systems, as well as privately-owned devices using the University's networks and resources. The policies apply to technology administered by individual departments, to information services hosted by dorm-resident students or by authorized resident visitors on their own hardware connected to the campus network, to the resources administered by central administrative departments such as University Libraries or OIT (Office of Information Technology), to authorized collaborative devices connected to the campus network and using University Internet addresses, to personally-owned devices connected by wire or wireless service to the campus network from University-owned housing or via campus locations providing mobile wired access or wireless access, and to actions originating from computer systems or mobile devices maintained or used by members of the campus community off-campus, but connecting remotely to the University's network services and under the aegis of the University's name. The policies also apply to actions of visitors to the campus who avail themselves of the University's temporary visitor wireless network access service and those who register their computers and other devices through Conference and Events Services programs or through other offices, for use of the campus network.

Privately-owned computer systems or mobile devices, or those owned by collaborative research projects, when attached to, or connected via, the campus data network and/or other campus resources, are subject to the same responsibilities and regulations as pertain to

University-owned devices and systems. University account holders including departmental computer users with University accounts who use computers or mobile devices belonging to others to connect to the campus network either directly or via Virtual Private Network (VPN) must assure that the devices are in compliance with University regulations before making such connections, except when accessing only Princeton University public World-Wide Websites from the outside device.

In general, as stated in Rights, Rules, Responsibilities, the University normally does not impose penalties for misconduct off campus beyond the local vicinity. However, electronic misconduct directed by a member of the Princeton University community against another member or members of the Princeton community may be actionable regardless of the network or devices used or the location from which the misconduct originated. As per RRR, judgments about such incidents will depend on the facts of an individual case.

### **Penalties**

All faculty, students, staff, departmental computer users, and authorized visitors, and others who may be granted use of the University's systems and network services, must comply with the University's policies. When a member of the University community is found to be in violation of policy, any disciplinary action is handled by the normal University authority and via the normal disciplinary process that would apply for other types of infractions. When an authorized visitor or departmental computing user is in violation of policy, the University sponsor or host may be held accountable. If the matter involves illegal action, law enforcement agencies may become involved as they would for campus actions that do not involve the information technologies or Internet.

## ***Appropriate use of Princeton University IT resources***

### **Business use**

As a member of the University community, you are provided with the use of scholarly and/or work-related tools, including (but not confined to) access to the Library and its systems, to certain computer systems, servers, software, printers, services, databases and electronic publications; to the campus telephone and voice mail systems; and to the Internet. As a general matter, your use of such information technology should be for purposes that are consistent with the business and mission of the University.

Computing and network equipment and mobile devices purchased by the University remain the property of the University even if they are dedicated for your use. Equipment purchased under research or other grants normally is vested with the University though it is to be used for the purposes of the grant. When University-owned equipment no longer is needed, its disposition must be in compliance with University policy and may not be determined independently by the user of the equipment.

Tampering with University-owned IT equipment, including cell or smart phones, is defined as making unauthorized changes to the hardware or system-level software that may be in conflict with license or may void applicable warranties. University employees must not perform or condone such actions.

### **Personal use**

Personal use of these systems, except for students enrolled at the University, should be incidental and kept to a minimum. For example, use of such resources by an employee for other than work-related matters should be reasonable and limited so that it does not incur additional cost to the University, does not prevent the employee from attending to and completing work effectively and efficiently, and does not preclude others with work-related needs from using the resources, including the shared campus and Internet bandwidth. Individual departments or units may place additional restrictions on personal use of the resources by their employees.

### ***University access; your right to privacy***

#### **The University's right to access files**

All contents in storage on data and voice systems are subject to the rules of Princeton University, including the University's ability under certain circumstances to access, restrict, monitor and regulate the systems that support and contain them. In general, and subject to applicable law, the University reserves the right to access files and documents (including e-mail and voice mail) residing on University-owned equipment. All contents in storage on data and voice systems are subject to the rules of Princeton University, including the University's ability under certain circumstances to access, restrict, monitor and regulate the systems that support and contain them. This includes access without notice, where warranted. Non-intrusive monitoring of campus network traffic occurs routinely, to assure acceptable performance and to identify and resolve problems. If problem traffic patterns suggest that system or network security, integrity, or performance has been compromised, network systems staff will investigate and protective restrictions may be applied until the condition has been rectified.

Some departments that maintain servers or internal networks also collect usage data and may monitor such servers or networks to ensure adequate technical performance. Departments that collect such data are expected to protect the privacy of those using the resources. It is also important to note that the University may be required to produce such data in compliance with a valid subpoena or court order.

#### **Degrees of privacy**

Students, for whom the University effectively is a residence during the academic year, normally are afforded a high degree of privacy. University employees, who are provided with the use of

University resources for work-related purposes, are afforded a lesser degree of privacy as they may be directed to share certain work files and information with others or to make a computer account accessible to a supervisor to assure effective backup or execution of the work when no other practical means exist for sharing the needed information readily and securely. In the event that business-related files (including e-mail) stored on an employee's account or workstation, or voice mail stored under the employee's telephone number, must be accessed, whether because of unexpected absence, death, or termination of employment, or other necessity, such files may be accessed and viewed, or accessed and heard, by the employing department. On employee termination, supervisors are expected to assure that passwords to computers, other networked devices, and accounts are obtained and changed if the work of the unit requires access to data or resources previously managed by the employee.

### **Others' files**

If you are a supervisor who has access to an employee's files or e-mail, or have been designated by a supervisor to access another employee's files or e-mail, you should be careful to avoid reading personal items that may be stored in the same area. For example, upon learning that an e-mail or voice-mail message is personal, and not business related, the supervisor or designee should immediately exit the file, e-mail, or voice mail message. The supervisor or designate should be careful to avoid examining any personal information the University may provide to the employee via password access, such as benefits or payroll data. When an employee leaves the University, the employee normally should be given the opportunity to remove any personal files or e-mail from University computers and other University-owned networked devices before departure. Departing employees are not entitled to remove, destroy or copy any of the business-related documents entrusted to their care or created by them during their employment, unless otherwise permitted by the University. The University's Record Retention Policy also must be observed. The University Record Retention Policy may be seen at <http://www.princeton.edu/records>. Where the Office of the General Counsel has issued a "Legal Hold Notice," individuals may be required to suspend regular retention practices and to retain information until further notice from Office of the General Counsel, including after an employee's departure from the University.

### **Disclosure**

In addition to information you may store on computers owned by the University, the University maintains certain system backups and logs of e-mail and network transactions. If the University is presented with a valid subpoena or court order requiring that such information be produced (or preserved), or directing that the University assure that its employees produce (or preserve) such information, the University may be bound by law to comply. Similarly, the University also may be obligated to disclose the identity of an account-holder or identity of the person who owns a computer or other registered network device, is responsible for a University-owned computer or networked device, or holds a University-assigned account used in some electronic transaction.

Supervisors are encouraged to set reasonable expectations for their employees regarding privacy of employee files and e-mail, and to remind employees of these expectations

periodically. Supervisors also are expected to take prompt action to retrieve or preserve employee files needed to continue the work of the department when an employee is about to separate from the University.

## ***Managing electronic information (including e-mail)***

### **Retention and disposal**

Employees of the University should understand that electronic information is governed by the same laws and regulations as are paper documents, including statutes protecting the privacy of student records, medical information, and personally identifiable information. Employees are expected to apply to electronic information the same record retention practices applied to paper documents.

Employees are responsible for retaining information that is of value to the University, whether that is for business processes for legal purposes, or historical value. The University has a Record Retention Policy (<http://www.princeton.edu/records>) offering recommended retention periods for common University records. Disposition of records created, retained or stored in information systems, computers, other networked devices, mobile devices, external storage services, or stand-alone storage devices should proceed on the same basis as for traditional paper records.

E-mail should be handled as any other correspondence in terms of retention and disposal. There are three ways of preserving e-mail: on the e-mail system, within an office's paper files, or in some form of electronic record keeping system, for example OnBase. As a general rule, the longer the message must be maintained or the more it need to be shared, the greater the need to remove it from the e-mail system and store it as hard copy (including the metadata accompanying the message) or in an electronic record keeping system. Attachments must also be identified and linked to the original message so that they may be easily located. Regardless of the methodology chosen, the authenticity and integrity of the entire e-mail message should be preserved.

Generally speaking, e-mail systems are communication systems, not record keeping systems, and are not designed for the efficient management or preservation of messages stored on them. Storage of e-mail to some form of record-keeping application most fully satisfies the need of current access to e-mail and also enhances value by allowing searching and sorting, maintaining linkages, and allowing for the full integration of the e-mail file into the offices' workflow processes. Such systems also offer the potential for preserving and making accessible records scheduled for long-term retention. E-mail retained in electronic format must be migrated to new software and storage media as upgrades occur.

Like all records, e-mail eventually will cease to be useful to the office, and at this point should be deleted from the inbox and/or sent folders. Then the "Trash" or "Deleted Items" folder

must be emptied (either manually or on an automated schedule) to properly dispose of the e-mail record. Then the records truly are deleted. (While it may be possible for a specialist to reconstruct the deleted files, it is not necessary for you to do anything further.)

When you trade in or replace a computer or other networked device, it is required that you or your computing support specialist use appropriate effective software to remove any and all data from the hard drive, or if warranted, destroy the hard drive by means approved by the University's Information Security Officer. As with the disposition of any other University records, e-mail disposal should be regularized and documented. With respect to back-up media, it is recommended that these storage devices be physically destroyed when no longer needed.

### **Official e-mail**

You are responsible for knowing the content of important e-mail communications sent to you by University officials.

### **Outside e-mail**

Faculty and staff who have e-mail accounts with services outside the University are encouraged to use only their University-managed e-mail accounts for communications regarding University matters to better protect the privacy and security of University data. Moreover, use of University-managed e-mail accounts will facilitate responses to subpoenas and other situations that may require the retrieval, inspection or production of documents including e-mail.

Princeton account-holders who have their e-mail copied or forwarded to an outside account must take care to avoid marking any such copied or forwarded mail as spam. Major Internet service providers have barred all e-mail coming from the Princeton domain when the provider's customers have marked as spam what the provider perceives to be too many messages. Such incidents can interfere with the business of the University as well as impede communication for members of the University community.

### **Protecting data**

You are responsible for assuring that there are backups of important documents and files which reside on systems supported by the University, and for protection against unauthorized access to, sharing, or viewing of, any sensitive information or any copyrighted material stored on your networked device or account.

If you have authorized or inadvertent access to sensitive or confidential data, you must observe the University's Information Security Policy ([www.princeton.edu/informationsecurity](http://www.princeton.edu/informationsecurity)) and know which University office has stewardship of, and authority over, the information. Any handling of such data, whether in hard-copy form, on University-owned equipment, or via personally-owned home devices, should be done in the most secure confidential manner. In the event of unauthorized access to University data, whether through theft or loss of portable devices such as USB drives, laptops, smart phones or other devices, or any other kind

of breach of security, the individual who possessed the device or learns of the breach is responsible for notifying the appropriate University offices of a potential data breach, and assisting with the University's data breach response (<http://www.princeton.edu/itsecurity/what-to-do-if/databreach/>).

Sensitive data should not be stored on laptop computers, flash drives, smart phones, or other devices that are easy to carry away. If it is absolutely necessary to store sensitive or confidential information on such a device, the information must be encrypted to protect it from view should the device fall into unauthorized hands. It also is essential to provide adequate physical security for any device, including a desktop machine that contains sensitive data. The University-endorsed encryption product or protocol should be used whenever possible. If the University has not yet endorsed a particular product or protocol for the platform you use, you should be prepared to use one when it is announced as endorsed.

Those who travel on University business should know that some encryption software may not be taken out of the United States. For that reason, and to avoid transporting unneeded University data, it may be prudent to travel with a computer or mobile device specially configured for travel rather than with the laptop or mobile device used locally at Princeton.

If you are responsible for data that are important to the University and that are created or stored on portable devices, you also are responsible for ensuring that the information is backed up regularly in a form that permits ready retrieval.

The advent of storage services in "the cloud" (for example DropBox) provides a tempting alternative for those who use portable network devices or have computers stationary in several locations. However, the security of such services has yet to stand the test of time. Unless the University can establish or recommend a particular service, your storing confidential or sensitive University information in such a "cloud" service poses serious risks, analogous to storing such information unencrypted on a readily-portable device.

The Princeton Desktop Council (DeSC) has indicated that peer-to-peer file-sharing software may not be installed or used on Princeton's DeSC computers because such applications could expose to Internet access information that is sensitive, confidential, or University-private.

The "people search" facility on the Princeton University home page returns an acceptable use policy statement with the results of a search. The statement is intended to prevent misuse of contact information by marketers and others. If a department provides a "people search" feature as part of a departmental website, it should include a similar statement.

## ***Protecting the University's good name***

### **Good judgment**

You are responsible for knowing the regulations and policies of the University that apply to appropriate use of University technologies and resources. You are responsible for exercising good judgment in use of the University's technological and information resources.

As a representative of the Princeton University community, you are expected to respect the University's good name in your electronic dealings with those both within and outside the University.

### **Use of the name**

As stated in *RRR*, "No individual or organization of the University may use the name Princeton University or a name that suggests Princeton University, or the name of any Princeton University organization, except to the extent such individual or organization has been officially recognized by the proper University authorities or as permitted under trademark law." Deliberate misuse of the name of the University by any member of the University community will be regarded as a serious offense.

### **Directory use**

Information in Princeton University's on-line campus directory is provided solely for use by members of the Princeton University community and by others who wish to reach a specific individual or resource at the University. Use of the information for solicitation by mail, e-mail, telephone, or other means, or for creation of a database for such use or for other purposes, is prohibited. Any member of the University community who misuses the data in such a way may be subject to disciplinary action.

### **Enabling others**

The privilege of using University equipment, wiring, wireless access, computer and network systems and servers, broadcast media, and access to global communications and information resources is provided by the University and may not be transferred or extended by members of the campus community to people or groups outside the University, without authorization. This includes providing network service to others through your own University network connection. Network service to residential units leased by the University may be extended to sublessors only when University Housing has approved the sublease.

If you administer a server or allow accounts or access for others, whether members of the University community or people outside Princeton University on a system you own or control, you are responsible for protecting the University's property, license agreements, and good name from damage by others to whom you might provide access. You also are responsible for assuring that no copyrighted material (including music, film or television, podcasts, computer games, and software) is published on, or distributed from, that system without permission of the copyright holder. If you cannot accept such responsibility, you ought not be providing

access for others. You are responsible for assuring that a strong root or administrative password is in place; for installing and maintaining appropriate anti-virus and firewall protections; for being aware of known vulnerabilities and for ensuring that the system you own or administer is not used by outsiders to relay commercial or other unsolicited mass e-mailings ("spam"); and, in general, for securing the system and its services against use by viruses, worms, or outsiders for attacks on other systems within, and outside, the Princeton University domain, or for other hostile or abusive purpose.

## ***Civility and respect for others***

### **Civil behavior**

Actions that make the campus intimidating, threatening, demeaning or hostile for another person are considered serious offenses by the University. Contemporary technology makes it possible for mistakes to be made more rapidly, and spread more widely, than ever before.

When you compose, send, or redistribute electronic mail or voice mail, when you create or publish postings to World Wide Web pages (including images, message boards, social network sites, Twitter, or chat rooms), or mailing lists, or produce and submit for campus broadcast video materials, consider whether you would make identical statements face to face with the person or people who may read, hear or view your work. The same principles pertain regarding people or groups you may address outside the Princeton University community as to those within.

As stated in *Rights, Rules, Responsibilities*:

"Respect for the rights, privileges, and sensibilities of each other is essential in preserving the spirit of community at Princeton. Actions which make the atmosphere intimidating, threatening, or hostile to individuals are therefore regarded as serious offenses. Abusive or harassing behavior, verbal or physical, which demeans, intimidates, threatens, or injures another because of his or her personal characteristics or beliefs or their expression is subject to University disciplinary sanctions...."

### **Photo devices**

Surveillance cameras and other such devices should not be used in places or ways that violate a reasonable expectation of privacy on the part of those whose activities are to be monitored or recorded. Locker rooms, restrooms, personal residences or dormitory rooms are some of the places where persons reasonably have an expectation of privacy, and in which adequate notice and consent of the subject(s) should precede the use of any photographic or sound recording device. Capture and dissemination of images and sounds in such situations without such notice and consent of the subject(s) is disrespectful of their rights and may violate University policy.

### **Harassment and defamation**

When using the campus technologies or access to network technologies provided by the University under its name, or in any other venue in which you are acting as an agent of the

University, you must refrain from creating and sending, posting, or displaying, or causing to be sent or posted, or displayed, or assisting to create and send or cause to be sent, posted, or displayed, any malicious, harassing, or defamatory messages or statements regarding another person, via e-mail, instant message, text message, Twitter or voice mail, by posting to message boards, mailing lists, social networks or newsgroups, by posting to the World Wide Web, by issuing as a virtual reality avatar, or by inclusion in a video produced for broadcast via the campus network, TigerTV, or YouTube or similar service.

You must be sensitive to the public nature of shared facilities, and take care not to display on workstations in such locations inappropriate images, sounds or messages which could create an atmosphere of menace or harassment for others.

You also must refrain from transmitting to others in any location inappropriate images, sounds or messages that are clearly threatening, hostile, or harassing in contradiction to the code of civility defined in *RRR*. If the deliberate use of anonymity or pseudonymity in electronic communication is for fraudulent purposes or accomplished with the intent to harass another, misrepresent oneself as another, or any other behavior in conflict with *RRR*, it will be considered a serious transgression.

## ***Use of the technology for commerce or solicitation***

### **Commerce**

Members of the University community are prohibited from using University computer resources for commercial purposes. Campus-based organizations claiming national or regional status must use non-University electronic resources, including Internet access, for non-Princeton activities.

University departments and groups that are authorized to conduct certain kinds of commerce and who take credit card information over the campus network or Internet must comply with University policies and other standards related to such e-commerce. See <http://www.princeton.edu/itsecurity/policies/CreditDebitCardPolicy.pdf>.

### **Solicitation**

Electronic mail or World Wide Web or newsgroup solicitation for fund-raising, even on behalf of non-profit organizations, also is prohibited.

### **Commercial links**

If you link to a commercial site from your Princeton University personal web page, you must take care not to do so in a manner that suggests the commercial site has the endorsement or support of the University.

If you maintain an outside website (.org, .net, .com, or other) that you wish to redirect to a Princeton University web page, you must do so in a manner that will not suggest the University sponsors, endorses, or otherwise supports the outside site. If an outside contractor maintains a website that you want to appear to be a Princeton University website, you must obtain approval from the Office of the General Counsel.

If you maintain an outside website that you want to present or otherwise identify as a Princeton University website or affiliate, special authorization is needed. This normally requires review by the Office of the General Counsel. The same is true if you want to create a website internal to Princeton that is intended to represent an outside group or activity unaffiliated with the University. In this latter case, the group or sponsoring organization also must agree.

## ***Use of the technology for political activity***

### **Political campaigns**

Members of the University community, as individuals and groups, have the right to exercise their full freedom of expression and association. However, as a Section 501(c)(3) organization, the University is prohibited from participating or intervening in any political campaign on behalf of or in opposition to a candidate for public office. In order to constitute participation or intervention in a political campaign, the activity must be that of the University and not the individual activity of its faculty, staff or students.

A website is a form of communication. If the University were to post something on its website that favored or opposed a candidate for public office, it would constitute prohibited political activity. It is the same as if the University distributed printed material, or made oral statements or broadcasts that favored or opposed a candidate.

Similarly, individuals may not use the technological resources of the University for political purposes in a manner that suggests the University itself is participating in campaign activity.

### **Other political activity**

In using University resources with respect to other political activity, individuals and groups should take care to make it clear that when expressing political views they are speaking only for themselves and not for the University. Non-partisan educational activity is acceptable.

## ***Your responsibility for network and information security***

### **Protecting accounts**

If, because of your status as a member of the University's student body, faculty or staff, whether active or on leave, or as an affiliate, departmental computer user, or authorized visitor, or as the representative of an authorized University group, the University has provided you with a computer account that provides access to the University's computer systems, networks, voice mail services or other technological facilities, you are accountable to the

University for all actions that are performed by anyone who uses that account. Therefore, you are expected to take reasonable measures to prevent your accounts from being used by others. Since passwords are a primary method of protecting University systems against unauthorized use, you, as a University-provided account holder, are expected to change any pre-assigned default password at the first possible opportunity, to select strong passwords that are difficult to guess, and to safeguard them from casual observation or capture. Thereafter, it is strongly recommended that passwords be changed at least once a year (ideally more often). Intentional sharing of such passwords with associates, friends, or family is prohibited, unless required by the terms of University employment or the nature of the group to which the account has been assigned. If there are alternate and practical ways to share work-related information readily and securely, these should be used rather than one University employee's being given the password of another.

An enhanced security profile (ESP) is a primary method of protecting access to some University services and data. As an account-holder, you are expected to protect the answers to your ESP security questions as you would protect your password.

There are Internet services designed to allow you to store personal information such as passwords, PIN numbers, credit card numbers and other data for ready retrieval by smart phone or other mobile device. If you elect to store your University password(s) through such a service, you risk exposure and subsequent misuse of your University account access and files.

### **Allowing access to others**

If you administer a server or allow accounts or access for others, whether members of the University community or people outside Princeton University on a system you own or control, you are responsible for protecting the University's property, license agreements, and good name from damage by others to whom you might provide access. You also are responsible for assuring that no copyrighted material (including music, film or television, podcasts, computer games, and software) is published on, or distributed from, that system without permission of the copyright holder. If you cannot accept such responsibility, you ought not be providing access for others. You are responsible for assuring that a strong root or administrative password is in place; for installing and maintaining appropriate anti-virus and firewall protections; for being aware of known vulnerabilities and for ensuring that the system you own or administer is not used by outsiders to relay commercial or other unsolicited mass e-mailings ("spam"); and, in general, for securing the system and its services against use by viruses, worms, or outsiders for attacks on other systems within, and outside, the Princeton University domain, or for other hostile or abusive purpose.

### **Securing Web-based applications**

If you are responsible for any web-based application presented through the University's resources, you must ensure that it cannot be used by anyone to relay unsolicited e-mail or spam to others. You also must ensure that the application cannot be used by others to compromise the application itself or the server on which the application resides.

Applications provided through cPanel or similar services on a University-maintained device will be scanned for vulnerabilities before being made operational, and any vulnerabilities should be addressed. If serious vulnerabilities in such an application are observed after initial implementation, the application must be removed until the vulnerabilities have been remedied.

Applications downloaded for mobile devices may also pose security risks and should be installed only when there is confidence they are secure.

### **Discovering gaps in security**

If you encounter or observe a gap in system or network security, you must report the gap to the appropriate office or authority, which may be the OIT Help Desk, the Library Systems Office, or the appropriate system authority, either within or outside the University. (The website [www.princeton.edu/itsecurity](http://www.princeton.edu/itsecurity) may be of help identifying the appropriate office.) You must refrain from exploiting any such gaps in security.

## ***Your responsibility regarding shared IT resources***

### **Appropriate use of shared resources**

The technological resources centrally administered by the Office of Information Technology (OIT) or University Libraries, and the distributed resources provided by individual academic and administrative departments of the University are intended to be used for educational purposes and to carry out the legitimate business of the University. Such resources include campus-public and department-private computer clusters, the University's World Wide Web server, departmental Web and file servers, Blackboard course management system, access to research databases, local-area departmental networks, the campus broadband and optical fiber network and global and Intranet network access, the University telephone and voice mail systems, general University multi-user computer systems and servers, individual departmental systems and servers, the campus Fax gateway, Second Life, TigerTV, Dormnet and access to Dorm video, Princeton's central and departmental e-mail service, and other shared campus facilities and services.

Appropriate use of such resources includes instruction, independent study, authorized research, independent research, and the official work of the offices, departments, recognized student and campus organizations, and agencies of the University. All of these activities rely on reasonable performance from the component units and the connections that allow interchange among them, and on the security and integrity of the resources. For these reasons, and because there often are times when some resources are in shorter supply than can easily meet the demand, certain performance-related or sharing guidelines pertain.

OIT and other University departments that operate and maintain computer and/or network systems and/or servers are expected to sustain an acceptable level of performance and must

assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for the others who rely on such services.

Devices that are badly configured or that have been compromised sometimes behave in ways that disrupt network service for others. In such cases, service to the device may be blocked, or the device may be marked ineligible for network access, until the responsible party can be contacted to take corrective action.

Researchers and students with network experiments should not plan to use the University's production network services for their research without authorization, and should understand that disruption of normal network service will not be permitted.

Users of shared resources should be careful to avoid making available via those resources items that are prone to excessive or other uses that may degrade or otherwise compromise performance. If a research project requires very large amounts of a resource, the researcher may need to make special arrangements in advance of conducting the research.

### **Library resources**

Many of the databases, electronic periodicals and other publications that the University offers through its libraries are subject to license agreements with outside vendors that impose restrictions on your use of these resources. For example, such licenses often limit the number of documents that you may scan or the number of pages you may print. Violations of such restrictions can result in the termination of licenses and the loss of access to resources that are important to the University's mission. Before using such licensed resources, you will be given notice of any relevant restrictions and are responsible for complying with them at all times.

### **Collaborative projects**

There are national and international projects that rely on cooperation and collaboration of large numbers of computer systems to conduct research. You may not use your account on central University shared servers to cooperate in such projects, though you may elect to use a personally-owned device connected to the campus network so long as the quantity of data transmitted does not affect network performance adversely for the rest of the campus. Some departments may also give permission for their locally controlled computers to be used for such a purpose. Some cooperative projects, for example the TOR project, carry the risk of the Princeton participant's device's being in violation of University policy because of the nature or content of network traffic passing through the device, particularly if it serves as an exit node.

Those wishing to participate in such projects should be cautious for this reason and may be asked to withdraw from participation if violation of University policies occurs.

### **Temporary visitor access to IT resources**

The University provides temporary visitor wireless network access service primarily for use by conference attendees, visiting colleagues from other schools, vendors making presentations, and other visitors with computers or other devices equipped for wireless access and who do not want or need to register their computers, smart phones, or other devices for more frequent

network service. The temporary visitor wireless network access is not intended to provide service to devices used regularly on campus by Princeton University faculty, staff, or students, or to longer-term visitors. Such devices must be registered properly for network connectivity. Members of the University community may use the temporary visitor network access with other wireless-enabled devices, provided the frequency of use is no greater than seven days in a calendar month and the devices are not disruptive to network availability and performance. Temporary visitors and members of the University community who use the visitor wireless service must comply with University policies regarding network and Internet use. Abusive behaviors that disrupt campus service can result in a device's being blocked indefinitely from further use of any University network services.

### **Mass mailings**

At Princeton, very large mass electronic mailings or voice mail broadcasts are permitted only by authority of appropriate University offices. The same authority would govern e-mail to those constituencies, even if the sender does not use the official list, but creates multiple smaller groups to accomplish the same end. In general, the same authority approves the use of large e-mail lists as approves large paper mailings to the same audiences. You may not send large mass e-mailings or voice mailings without the appropriate University authorization.

Appropriate authorization also must be obtained to conduct Web-based or e-mail surveys, whether among members of the campus community or of people outside the University. Surveys related to research and instruction must obtain approval from the University's Institutional Review Panel on Human Subjects, and, in the case of undergraduate research, from Office of Dean of the College. Special approval is not needed for departments seeking feedback on their courses or services, nor for recognized organizations canvassing their members.

"Spamming" is spreading electronic messages or postings widely and without good purpose. "Bombing," sometimes known as "spamming" as well, is bombarding an individual, group, or system with numerous repeated messages. Both actions interfere with system and network performance and may be harassing to the victims, which in the case of newsgroups can number in the thousands. Both are violations of University regulations. Sometimes, people spam unintentionally. If e-mail is sent to a large list of people with all the addresses visible (rather than blind-copied or via a group list) and someone accidentally replies to "all," rather than just to the sender, the reply with irrelevant information is copied to everyone on the list. Deliberate replies of this nature will be considered a violation of University regulations.

### **Use of limited resources**

You must refrain from unwarranted or excessive amounts of storage on central or departmental computing systems and servers, and from running grossly inefficient programs when efficient ones are available unless the responsible departmental authority has directed or approved such use for specific instructional or research applications.

You must refrain from running servers or daemons without prior permission on shared systems you do not administer.

You must be sensitive to special need for software and services available in only one location, and cede place to those whose work requires the special items.

You must not prevent others from using shared resources by running unattended processes or placing signs on devices to "reserve" them without authorization. Your absence from a public computer or workstation should be no longer than warranted by a visit to the nearest restroom. A device unattended for more than fifteen minutes may be assumed to be available for use, and any process running on that device terminated. You must not lock a workstation or computer that is in a public facility. You must also be sensitive to performance effects of remote login to shared workstations. When there is a conflict, priority for use of the device must go to the person seated at the keyboard rather than to someone logged on remotely.

You must consider the shared nature of the campus network bandwidth, and be careful to avoid transmitting large amounts of data unnecessarily. Providing servers on personally owned computers connected to the campus network can have an adverse influence on general network performance if large files are delivered or if many hundreds of people attempt to obtain the files concurrently. If you use peer-to-peer sharing applications you must limit uploads to no more than one at a time (ideally, to zero), to prevent excessive use of Princeton's Internet bandwidth by others on the Internet, and you must comply with copyright regulations.

Because the University's Internet connectivity is a limited resource, only devices that must permit multiple concurrent uploads in support of instruction or other University business will be permitted to allow more than one upload at a time. Other devices on the University network that serve files to the Internet must limit uploads to only one file at a time. (Web pages normally need not be restricted in this way, provided they are not also acting as file servers.)

Where the University has obtained very limited licenses for software, you must use only one share, not several concurrently.

You must avoid tying up shared computing resources for excessive game playing or other trivial applications.

### **Paper and printing resources**

Unnecessary printing is wasteful in dollar cost and is in conflict with the University's sustainability goals. Members of the University community should practice thrifty and judicious printing. When a work is in progress, editing should take place on-line whenever possible rather than on a printed draft. Information that can be shared effectively electronically should not be printed at all. When it is necessary to print notes or reference material, consideration should be given to placing multiple pages on each sheet of paper and using two-sided (duplex) printing whenever possible.

If someone without appropriate authorization removes paper from departmental printers or copiers, or from computer clusters, to use for printing or copying elsewhere or for any other purpose, it will be considered a disciplinary matter.

### ***Ensuring network performance***

You must not attempt to intercept, capture, alter, or interfere in any way with information on local, campus or global network pathways. This also means you may not run "sniffers" (programs used illegitimately to capture information being transmitted) on the campus network or any portion thereof. You may not operate Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BootP) servers on the campus networks without authorization.

You must not attempt to obtain system privileges to which you are not entitled, whether on Princeton University computers or on systems outside the University. Attempts to do so will be considered serious transgressions.

Computer procedures, programs and scripts that permit unauthenticated or unauthorized senders to send e-mail to arbitrary recipients from unrestricted sources are prohibited.

You must refrain from any action that interferes with the supervisory or accounting functions of the systems or that is likely to have such effects. You must refrain from creating and/or implementing code intended to periodically or aperiodically interrupt or interfere with computer systems or services. You must refrain from knowing propagation of computer viruses or presumed computer viruses. You must not conduct unauthorized port scans. You must not initiate nuisance or denial-of-service attacks, nor respond to these in kind.

Individual members of the campus community who elect to install wireless access points must assure that their operation will not disrupt University wireless network service. If the access point is installed and configured as a "bridge," the people responsible for the systems using that device for network access will remain responsible for activity from their respective devices. If the wireless access point is configured as a "NAT" (Network Address Translator), the person responsible for the NAT will also be held accountable for all activity by those using the NAT.

Wireless access points may not be installed by individuals in campus academic, administrative, or service buildings, including buildings rented or owned by the University off campus without authorization from the department responsible for the area involved. If authorization is provided, the individual must comply with any rules regarding the wireless access point established by the department.

Wireless access service is provided by the University in campus dormitories and some University-owned off-campus apartments. Some commonly used appliances, for example

certain cordless telephones and most microwave ovens, operate at a frequency that could interfere with wireless network service. Personal wireless access points also can cause such interference. If a device interferes significantly with the University's residential wireless network service, the owner may be required to relinquish use of the device in the residence. Malicious use of any such device to disrupt network service will be considered a serious violation of University regulations.

Computers, smart phones, and other network devices connected to the University's network must be registered for network use. Each will be assigned an Internet Protocol (IP) address or, if mobile, "leased" an address by the University's network management servers. Using other than the assigned IP address can disrupt normal network operation for others, so users and owners of such devices are expected to refrain from supplying some other IP address for use in any network transaction.

Individuals may not operate their own network management servers (DHCP or BootP) on the campus network, as such rogue servers quickly can disrupt network service to others. Such a server may be connected to a private network within the Princeton.EDU domain, but only if the reply packets sent by the server are confined to the private network and do not enter the campus network at any time.

## ***Honesty, integrity, and the law***

### **The law**

The University is expected to uphold local, state and federal law, including copyright law.

Members of the University community may not knowingly assist others with use of the University's information technology resources or Internet access for purposes of violating the law, including copyright law. Employees who are asked for such assistance must refuse.

Moreover, an employee should report suspicion of crime involving, or revealed by, University technology resources (such as computers, mobile devices, network or Internet access, e-mail) to appropriate University officials. For example, if you are an employee and, during the course of your work, learn of criminal activity involving child pornography or offenses involving minors, you should bring this information to the attention of a supervisor. Department of Public Safety should be contacted immediately if the activity poses a risk of immediate harm to others. In all cases, employees must treat information regarding potentially unlawful activity with discretion and sensitivity to the privacy rights of others.

### **Dishonest actions**

There also are actions which may not be specifically prohibited by law, but which are nonetheless dishonest. *Rights, Rules, Responsibilities* states: "Members of the University

community are expected to be honest and straightforward in their official dealings with University processes, activities, and personnel. This obligation includes honoring contracts and agreements and providing accurate information on official forms and documents as well as to official University personnel, offices, and committees. Deliberate violations of this provision will be considered serious offenses; subsequent violations, or systematic violations in the first instance, will be considered extremely serious." Such actions also are unacceptable when conducted by means of the University information technology resources and Internet access.

You must not create, alter, or delete any electronic information contained in, or posted to, any campus computer or affiliated network for fraudulent or deceptive purposes that may be harmful to others. Moreover, signing an electronic document (including e-mail), or posting to a Website, message board, or social network, or appearing as a virtual reality avatar, with someone else's name may be a violation of University rules especially if the person whose name you are signing has not consented to your doing so. It also will be considered a violation of University rules if you use the University's electronic resources or Internet access to create, alter, or delete electronic information contained in or posted to any computer system on or outside the campus for which you are not authorized to do so.

Unauthorized attempts to browse, access, solicit, copy, use, modify, or delete electronic documents, files, passwords, images, films, music, sounds, games or programs belonging to other people, whether at Princeton or elsewhere, will be considered serious violations.

You must not use another's accountable resource or account-affiliated access or personal computer or networked device without authorization. If you encounter an open session that exposes another's accountable resource, close the session and try to notify the individual, whether within the Princeton.EDU domain or elsewhere on the Internet. It is considered a serious transgression to exploit the accidental exposure of another's account or to borrow or steal another's identity. Without authorization, you must not attempt to enter and listen to another person's voice mail, or enter and read another person's e-mail, or other electronic messages or files, even when these are accidentally exposed to your access. It is considered a very serious transgression to gain unauthorized access to another's accountable resources or another's personal device or workstation, e-mail, or files, through deliberate action.

You must not create and send, or forward, electronic chain letters. To do so may also violate federal law, even if the chain letter assures the reader that it is not illegal and cite statutes as "proof." The redistribution of chain letters is a violation of University policy even when there is no mention of money in the letter. Some chain letters which appear to relate to genuine causes often are "urban legend" by the time they reach you; if you research the issue you may discover the cause existed long ago and the letter no longer is meaningful.

You must not post "pyramid scheme" messages. A pyramid scheme calls for escalating numbers to send money, usually small amounts, to others, with the expectation that a large amount of money will come to them. Any posting or message that suggests such a scheme is a violation of University policy and may violate federal and other laws.

You may not “borrow” an Internet Protocol address assigned to another person or entity, create a fraudulent IP addresses for a device you own or are using, or attempt to use with one device the IP address assigned to another you own or use. You may not operate a server that assigns, or attempts to control, IP addresses on the campus network.

You may not falsify a hardware address for a device connecting to the campus network or a wireless interface used to connect a device to Princeton’s network.

Individuals registering a computer, smart phone, or other device for Dormnet or campus network service must provide accurate information about that device only, and must not attempt to obtain service for two separate devices simultaneously via a single registration.

You should be aware that there are federal, state and sometimes local laws that govern certain aspects of computer, broadcast video, and telecommunications use. With considerable focus on U. S. homeland security and the national infrastructure, and with escalating pursuit of copyright infringers continuing to generate concern, additional legislation is emerging. Members of the University community are expected to respect the federal, state and local laws in use of the campus technologies and University-provided network access, as well as to observe and respect University-specific rules and regulations.

### **Gambling**

Gambling is prohibited for employees in the workplace except as specifically noted in University policy 5.21 (<http://www.princeton.edu/hr/policies/conditions/5.1/5.1.1/>). This prohibition includes Internet gambling.

Internet gambling makes it possible for someone to gamble around the clock. Anyone who gambles frequently or for long periods of time may be gambling compulsively, which may damage his or her professional, academic, and personal life.

Gambling is a closely regulated activity in New Jersey, and to date none of the Internet gambling sites available in New Jersey are legal. Individuals who are defrauded or otherwise victimized in connection with their use of such sites are not likely to have any protection or recourse under New Jersey law. For further information regarding the risks and potential consequences of Internet gambling, see the website for New Jersey’s Division of Gaming Enforcement ([www.state.nj.us/lps/ge/internet\\_gambling/law.htm](http://www.state.nj.us/lps/ge/internet_gambling/law.htm)).

## ***Copyright and intellectual property***

### **Intellectual property**

Princeton University has a strong commitment to the protection of intellectual property rights. The widespread use of digital technologies has elevated a number of concerns in this area. Today's ease of access to information, images, musical recordings, films, videos, television shows, podcasts, software and other intellectual property does not mean that such materials are necessarily part of the public domain or otherwise free for use without authorization.

### **Copyright**

Members of the University community who engage in any activity that infringes copyright-protected materials may be subject to disciplinary action. Under circumstances involving repeated instances of infringement through the use of the University's computing network, such disciplinary action may include the termination or suspension of network privileges. For students, disciplinary action also may include disciplinary probation or greater penalty.

Those who violate copyright law may also be subject to civil claims for monetary damages and, in some cases, criminal penalties.

It is important to remember that copyright protection may apply even if you do not see the copyright symbol © or any other indication that the material in question has been officially registered with the United States Copyright Office. Infringement may be determined to have occurred if the copyrighted material is offered for unauthorized copy; actual distribution may not have had to occur.

More information on copyright law may be found at the website of the U.S. Copyright Office ([www.copyright.gov](http://www.copyright.gov)).

The rules of "fair use" pertain to Web and other electronic materials and media. Information about instructional use of copyrighted materials at Princeton may be found at this website (<http://www.princeton.edu/fairuse>).

### **Permissions for use**

If you want to use an object or work, which may include an image, a background pattern, a section of text or a musical, film, television show, or video selection that you would like to use, you should make a good faith effort to determine that such use constitutes a "fair use" under copyright law or you must obtain permission of the owner or copyright-holder. As a general matter, you are free to establish links to Web pages you enjoy and which you would like to share with others. But you are not generally free to copy or redistribute the work of others on World Wide Web (or elsewhere) without authorization and proper attribution.

If an individual who holds the rights to material has explicitly and intentionally established a World Wide Web page or a public server, or clearly designated a set of files as being for shared

public use, you may assume authorized access. Note that peer-to-peer file-sharing applications can establish shared space and share files without the conscious knowledge of the less technologically sophisticated user. Although it is the responsibility of the user of such software to take proper precautions, it also is abusive to exploit the opportunity such a lapse may present.

### **Restrictions**

It is your responsibility to restrict access to others' proprietary information that you may place on-line. For example, most popular peer-to-peer file-sharing software used to transfer music, film, video and other files among users, requires users to set certain protections explicitly. If someone fails to do so, anyone on the Internet can access without permission all files stored on the person's hard drive, and copyright infringement occurs.

The University makes available centrally through OIT and in distributed fashion through various academic and administrative departments, certain software for use by the campus community. In many cases, the license or contract covering the software states it may be used on the designated system, but that it may not be copied for use elsewhere, even elsewhere within the University. (This includes prohibitions against cross-assembly and reverse compilation.)

Many of the databases, electronic periodicals and other publications that the University offers through its libraries are subject to license agreements with outside vendors that impose restrictions on your use of these resources. Before using such licensed resources, you will be given notice of any relevant restrictions and are responsible for complying with them.

You are responsible for determining the restrictions on music files, video or television files, film files, podcasts, computer games, program, packages, and data before copying them in any form or permitting them to be copied by others. If it is not clear whether you have permission to copy such material, assume you are not permitted to do so. If you are given material by its creator or vendor, or by an instructor or supervisor, whether for test or for your use, do not assume the right of redistribution. Your physical possession of the property does not necessarily bring with it permission to pass it on to others. You may not circumvent copyright protection even on original media you own, to make copies of the material.

Some people believe there is no difference between taping a television show or using a service like Tivo to record it for later viewing, and downloading a copy of a television show from the Internet. There are several important differences, however, which may make the downloading a violation of copyright. Some people believe that, if they own a DVD of a film or television show, they can then download a copy legally under any circumstance. However, unless such copying has been authorized by the copyright holder or for some reason qualifies as a "fair use" under copyright law, the downloaded file is an infringing copy.

### **Attribution**

When doing academic work, you are responsible for properly attributing material--data, images, ideas, sounds, film, and verbatim text--that you find through electronic sources. The

University's requirements and standards for the acknowledgment of sources in academic work, found in *Rights, Rules, Responsibilities*, apply to all electronic media. At a minimum, you should provide a citation for an electronic source that includes the source's URL, author or site manager's name (if available) and the creation or download date.

### **Educational materials**

A faculty member who develops and uses electronic course materials, or a staff member creating training materials, should be familiar with, and observe, the Rules and Procedures of the Faculty or appropriate University regulations related to such materials.

### **Rights-holder concerns**

The entertainment industry in the United States has become quite vigilant in pursuing people who infringe copyright. The recording industry has established a website regarding legal and illegal sharing of music ([www.musicunited.org](http://www.musicunited.org)), and the Motion Picture Association of America has established a website related to film, television, and copyright ([www.respectcopyrights.org](http://www.respectcopyrights.org)). There is concern about copyright infringement as well among firms that produce software and computer games; literary agents regarding their clients' works; web designers; and photographers.

### ***Violations and penalties***

#### **University penalties**

As noted and defined in *Rights, Rules, Responsibilities*, for violations of University-wide rules of conduct, members of the community are subject to several kinds of penalties. The applicability and exact nature of each penalty vary for faculty, students, professional staff, and employees.

Members of the University community who engage in any activity that infringes copyright-protected materials may be subject to disciplinary action. Under circumstances involving repeated instances of infringement through the use of the University's computing network, such disciplinary action may include the termination or suspension of network privileges. For students, disciplinary action also may include any of the penalties outlined in *Rights, Rules, Responsibilities*.

Also, if an individual has used services provided by the University on a fee basis, but chose to evade payment of the fee, a penalty normally will involve paying the fee.

#### **Other penalties**

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than \$750 and not more than \$30,000 per work infringed. For "willful" infringement, a court may award up to \$150,000 per work infringed. A court can, in its discretion, also assess costs and attorney's fees. For details see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to \$250,000 per offense.

## ***Protection for you***

### **Phishing**

The growth of the Internet has brought with it increased opportunities for exploitation. Each day, billions of e-mail messages “phishing” for personal and financial information traverse Cyberspace. Despite all the warnings published by financial institutions and e-commerce enterprises and news coverage of such schemes, some people are fooled. People at the University have seen e-mail messages very cleverly designed to look as if they came from the Princeton University Credit Union. For tips on some of the dangers in Cyberspace, see the Information Security web page ([www.princeton.edu/protect](http://www.princeton.edu/protect)). When you are not sure whether such a message is genuine, it is appropriate and in fact preferable to check with a supervisor or other person in authority before responding or releasing information. It also may be appropriate to ask that the request for information be made in writing by mail or facsimile.

### **Social Engineering**

The term "social engineering" refers to more than technology. A scammer with a convincing line might telephone an office worker or student and claim to work for a Help Desk at Princeton or at some financial institution, and ask the person for his or her account and password for some plausible-sounding security purpose. It is important to use critical thinking skills even for telephone or live approaches from people you do not know.

### **Self-exposure**

Another type of danger is self-exposure. The rise of Facebook, MySpace, and other “social networks” encourages people to let their metaphoric hair down and to express themselves in ways that, in retrospect, might be a little too open for comfort. While communications or postings in the online facebook of a Princeton residential college are generally protected from the immediate view of the general public, statements made, and images published, on the Internet can typically be seen anywhere, can last essentially forever, and can have serious unintended consequences.

“Thoughts on Facebook,” (<http://www.cit.cornell.edu/policies/socialnetworking/facebook.cfm>), a Cornell University document presenting the issues, discusses the risks facing students who participate in on-line social networking, but similar cautions apply equally to employees who publish profiles on MySpace or similar venues.

Also: When creating public postings, tweets, or blogs of any kind, keep in mind the power of the World Wide Web to broadcast and preserve your statements. Any ill-considered postings may

survive your commitment to them, and, because of the distributed nature of Web indexing, may be very difficult to expunge in the future.

### **Where to turn**

The University is committed to protecting members of the campus community from abusive actions by others both within and outside the institution. If you experience abusive incidents related to the technologies that you cannot pursue on your own, or you are a supervisor who believes that an employee is abusing access to the information technology resources or Internet access, you should report the matter to the most appropriate contact. You also can report violations of privacy or property involving the technology, whether the perpetrator is a member of the campus community or not.

Among the many offices and officials that work together to pursue cases of this sort are the Deans, Directors of Student Life, and Directors of Studies at the residential colleges, Office of Dean of Undergraduate Students, Office of Vice President for Campus Life, the Graduate School Office, Office of Dean of the Faculty, Office of Human Resources, Ombudsman, University Health Services Counseling Center and SHARE Program, Office of Information Technology, Department of Public Safety, and Office of General Counsel.

If you do not feel your usual reporting path can work or are not sure of the appropriate division to handle the matter on your behalf, the OIT Help Desk will take your referral and see that it is directed appropriately. OIT Help Desk staff can also help you identify sources of harassing or offensive communications from outside the University network. You also can report "spamming" and abusive or offensive communications to outside authorities, as most schools, corporations, and Internet service providers do not intend their electronic resources to be used for nefarious purposes.

### ***Examples of acceptable behavior and policy violations***

#### **Access**

**Acceptable behavior:** A visiting relative is curious about Princeton's on-line services and Internet access. You demonstrate some of the facilities, and even let the visitor do some "hands-on" work, for example specifying some search terms for a World Wide Web search. You may also let the visitor check his or her own e-mail. But you are careful to retain control; you do not allow the visitor free rein, and may not allow the visitor to generate e-mail that will show a Princeton.EDU domain return address.

**Acceptable behavior:** A supervisor explains that others in the department may need to continue work on a particular document during your planned absence, and, if no alternate practical means of ready access are available, asks that you provide the account password for access to the document. You do so.

**Acceptable behavior:** A group of visiting scholars has arranged through Conference and Visitors Center to have University network access and NetIDs during their stay on campus.

**Violation:** You have a departmental computer account that provides access to certain shared files, to Princeton's general campus resources, to the Internet and World Wide Web. You do not use that account, and give the account and password to the director of a local community service agency, who uses it.

**Violation:** You have registered your device for the campus network. You are running a system that lets you set up e-mail accounts for other people. You want to offer free access to the device to people around the world with an interest in a specific public issue of great importance, and also give them e-mail accounts on your machine. (You can allow them access to information you have on your machine, provided it is not copyrighted by someone else, but it is a violation to extend to them e-mail accounts or access to other resources within the princeton.edu domain.)

**Violation:** Without University authorization, you use your campus-connected personal device to host a website, register a domain, or operate a mail-exchange server for a charitable or educational organization. (Hosting commercial sites or domains is expressly forbidden.)

**Violation:** You have discovered a new kind of peer-to-peer file-sharing software, and install it in space allocated to you on a shared central or departmental server. (To do so without violation, you would need permission from the unit responsible for the server—which is unlikely to be given.)

**Violation:** You expose your networked device to misuse by leaving it unattended (or otherwise unprotected) in a common area of your dorm room for an extended period of time.

### ***Copyright, IP***

**Acceptable behavior:** While browsing the World Wide Web, you find a table of information and are impressed by the presentation. You view the source data, and make a note of some of the commands the author used to create that display. You use some of the same commands to create a similar table, containing information you want to present via World Wide Web.

**Acceptable behavior:** You create a Web page, and include a link to someone else's Web page.

**Acceptable behavior:** You use a network sharing tool to download MP3 or other audio format music files for which you have obtained permission, or film or television files for which you have obtained permission, and you password-protect those files so no one without authorization can get them from your device, or you set an upload limit of zero in the application so no one on the Internet can get copies of your files.

**Acceptable behavior:** You are testing beta-release software, and know it could fix a problem a colleague is experiencing. You contact the manufacturer, and get permission to share the upgrade with your colleague, who already has a legally obtained copy of the current production product.

**Acceptable behavior:** You enjoy a song that is on a CD you bought or that you downloaded via a legal service such as iTunes, and you want to use it as a kind of personal theme song on your Princeton web page. You contact the agent of the artist who holds the copyright, and obtain permission to use the song in that fashion, giving proper credits as defined in your agreement with the artist's agent.

**Violation:** You have a legally obtained on-line copy of an audio format music file, or film or television show file. You have a network sharing tool empowered, which permits others around the world to upload copies of that file from your storage space, and you have put no protections in place to prevent uploading.

**Violation:** Episodes of a favorite TV show are made Web-available for viewing only via a network streaming site that is authorized by the copyright holder. Since the rights-holder is allowing anyone to view the episodes, you make a copy of your favorite and allow others on the Internet to share your copy.

**Violation:** You are asked by a computer manufacturer to participate in a beta test of a new operating system. You try it and it fixes many known problems. Without asking permission of the manufacturer, you put the software up on your server and post a message to a message board announcing that people may get a copy, free, at that location.

**Violation:** Your department has just added a new staff position. The individual hired into the position has a computer, but not a copy of the word-processing package you and the rest of the office use. The department does not have enough in the budget to buy another copy of the software, so you make a copy of your installation CDs for the new staff member to use. (If you have questions regarding the propriety of such action, contact the OIT Help Desk for guidance.)

**Violation:** You missed seeing a television show you like, and can't find a legal on-line source from which to view it, so you use a file-sharing tool like BitTorrent to find a copy on the Internet and download it so you can see it.

**Violation:** You subscribe to Netflix, but find the transmission slow, so you download a film to view via BitTorrent.

**Violation:** You create an electronic copy of a new novel and put it on-line, so you and your friends at other schools or in other places can look at the same text at the same time.

**Violation:** You bought a DVD of a recent film you like, but the disk was lost in an airport as you traveled. You later download another copy of the film from the Internet to replace the disk you lost.

## ***Harassment***

**Violation:** You live in the dorm; you and two friends are together, joking about a fourth person who seems to have a personal interest in you. You go into e-mail on your Dormnet device, create a sexually explicit message to the absent party, the person with the apparent personal interest. You have no intention of sending the message, but one of your visitors hits the "send" key. Both you and the person who caused the message to be sent will be held responsible for the incident.

**Violation:** You forward voice mail from another person to a voice list of twenty members, prefacing the voice-mail with the untruthful comment, "Just what you'd expect of someone who paid someone else to take his SAT exams for him!"

**Violation:** You and a friend are visiting a classmate at his home far from campus, and find the classmate's Gmail account open and active while the classmate is out of the room. You take the opportunity to look at the e-mail and images stored on the account, and to forward some of the most embarrassing to other Princetonians as if they came from the classmate.

**Acceptable behavior:** You are alone in a campus computer cluster, and use the computer to initiate some favorite music to provide background noise while you work. However, when other people arrive to use the cluster, you stop the music.

**Acceptable behavior:** You have an assignment that requires you to work with a collection of images some might find quite gruesome, and you need to use a computer in a campus cluster. You locate a machine that is situated in such a way as to protect others from inadvertently witnessing the images just by walking by.

**Violation:** You create or display in the workplace, on a device that others could or may see, an image that might reasonably be found offensive or inappropriate within the context of the workplace.

**Violation:** You change the system sound on residential college cluster computers to a potentially offensive or irritating noise.

**Violation:** You digitize an intimate photograph and install it as the background image on the workstations in a departmental cluster.

**Violation:** You e-mail or IM to another or others an image or joke that reasonably might be perceived by the recipient(s) as intimidating, hostile, threatening, or demeaning.

**Violation:** You use a public cluster to print a poster slandering an individual.

**Violation:** Knowing that your start-up screen or background display for the device on your dormitory room desk might be considered offensive by some, you nonetheless seek in-person help from a computing support person or residential computing assistant without suppressing the display.

### ***Mass mailings***

**Acceptable behavior:** You are an officer in a recognized campus organization, and (with approval from the appropriate University authority) send e-mail to all the members of the organization regarding a coming event.

**Acceptable behavior:** Someone "spams" you; you refrain from reply, but report the matter to the appropriate authority.

**Acceptable behavior:** You want to post a follow-up to an item on a message board you read, but you notice the previous poster has posted that item to several dozen message boards. You take action, which sends your posting only to the intended message board.

**Acceptable behavior:** On your personally owned device connected via the University network, you run a peer-to-peer application that allows you to set limits on uploads. You set the default upload limit to zero, so others on the Internet will not be using University bandwidth to get copies of files on your device's hard drive.

**Acceptable behavior:** You create and run a script that accepts information from a web form and sends the information to a set single address or fixed set of recipient addresses.

**Violation:** You create and/or run e-mail server software configured to accept e-mail messages from arbitrary senders and deliver to arbitrary recipients (an open relay).

**Violation:** Someone has "spammed" several electronic mailing lists to which you subscribe, so you "get him back" by sending seven hundred identical derisive mail messages to the person's e-mail address.

**About retaliation:** Retaliation in kind is not appropriate behavior, as it continues to victimize other people. There are appropriate avenues for protest, which will not violate University policy. See "Where to turn" in the section of this policy called "Protection for you."

### ***Commerce***

**Acceptable behavior:** Your recognized campus organization publishes Web pages. The group's home page contains this accurate information: "Membership in [name of group] requires payment of twenty dollars annual dues."

**Acceptable behavior:** You use e-mail to apply for a grant that will help pay for your textbooks and travel.

**Acceptable behavior:** Your offspring has outgrown the infant stroller and you want to sell it. You use your University access to post a "for sale" notice to the relevant message board.

**Acceptable behavior:** You are a student seeking summer employment, and use e-mail to communicate with prospective employers.

**Acceptable behavior:** You are about to graduate from Princeton, and use e-mail to communicate with potential employers.

**Acceptable behavior:** You are a faculty member whose scholarly publication is carried by an on-line bookseller; you make the book title on your web page serve as a "hot link" to the point of sale.

**Acceptable behavior:** Your recognized student organization has a CD that the group has been authorized to sell via the World Wide Web. You offer it for sale following the regulations for e-commerce established by the Treasurer's Office.

**Violation:** You are an officer in a recognized University organization that is supported by fees from members and "friends of" the organization. The organization has a WWW page explaining its activities. Rather than just state that support is by subscription from members and friends and stating factual information regarding fees, you post an appeal, "Send your dollars in now! Support this cause at Princeton."

**Violation:** You contract with a commercial firm to include a banner ad on your Princeton University personal home page, so that you will get a small payment each time someone connects to the company's site from the banner-link on your web page.

**Violation:** You are a University employee who manages a summer camp for children interested in chess. You use your Princeton University e-mail address and affiliation to advertise the camp.

**Violation:** You run an advertisement of your own for-pay service on your web page.

**Violation:** You use your networked device and assigned University IP address (Internet Protocol address) to register a domain and/or host a website or operate a mail-server with a .com designation.

**Violation:** Without University authorization, you provide a mail exchange agent (i.e., e-mail service) for a .org domain on a device connected to the University network.

**Violation:** You agree to let a commercial service use the excess capacity on your University-connected device as a network distribution point for files or services. (Such an agreement also entails use of the University's bandwidth, which you are not authorized to assign for such purposes.)

### ***Political activity***

**Acceptable behavior:** You use University equipment to videotape a debate between candidates for state office in order that a Politics class can view the video.

**Acceptable behavior:** You use your networked device to post to a non-University message board, expressing your view that a current candidate is the best candidate for a particular public office.

**Violation:** You use your University access to post to a message board indicating that Princeton University supports a current candidate for political office.

## Reviewers of the Princeton University IT Policy

Representatives from the following groups and University offices participated in review and development of the 2011-2012 University IT Policy:

Graduate School Office  
Graduate Student Government (GSG)  
Office of Dean of the College  
Office of Dean of the Faculty  
Office of Dean of Undergraduate Students  
Office of the General Counsel  
Office of Human Resources  
Office of Information Technology (OIT)  
Office of Vice President for Campus Life  
Residential Colleges Directors of Student Life and Deans  
Undergraduate Student Government (USG)  
University Libraries

### ***Added reading on related subjects***

Go to the [www.princeton.edu/itpolicy](http://www.princeton.edu/itpolicy) website, and link via the “Added reading” link within the left menu.