## Table of Contents

**Policy Statement** ............................................................................................................................. 1
**Introduction to Policy on Acceptable Use of Princeton University IT and Digital Resources** .......... 1
    - Reasons for this Policy .................................................................................................................. 2
    - Examples ...................................................................................................................................... 2
**Who must comply? What penalties pertain?** ................................................................................... 2
    - Compliance ................................................................................................................................. 2
    - Penalties ..................................................................................................................................... 3
**Appropriate use of Princeton University IT and digital resources** ...................................................... 4
    - Business use ............................................................................................................................. 4
    - Personal use ............................................................................................................................. 4
**University access; your right to privacy** ............................................................................................ 4
    - The University’s right to access files ....................................................................................... 5
    - Degrees of privacy .................................................................................................................... 5
    - Others’ files ............................................................................................................................. 6
    - Disclosure ................................................................................................................................. 6
**Managing electronic information (including e-mail)** ......................................................................... 7
    - Retention and disposal ............................................................................................................... 7
    - Official e-mail ........................................................................................................................... 8
    - Outside e-mail ............................................................................................................................ 8
    - Protecting data .......................................................................................................................... 8
**Protecting the University’s good name** ............................................................................................. 10
    - Good judgment .......................................................................................................................... 10
    - Use of the University’s name .................................................................................................. 10
    - Directory use ............................................................................................................................ 11
    - Enabling others ........................................................................................................................ 11
**Civility and respect for others** .......................................................................................................... 11
    - Civil behavior ........................................................................................................................... 11
    - Harassment and defamation ..................................................................................................... 12
**Use of technology for commerce or solicitation** ............................................................................ 12
    - Commerce ................................................................................................................................. 12
    - Solicitation ............................................................................................................................... 13
    - Commercial links ..................................................................................................................... 13
**Use of technology for political activity** ............................................................................................ 13
    - Political campaigns .................................................................................................................. 13
    - Other political activity ............................................................................................................. 14
**Your responsibility for network and information security** ................................................................. 14
    - Protecting accounts .................................................................................................................. 14
Additional reading on related subjects

Reviewers of this 2015-2016 policy

Additional reading on related subjects
Acceptable Use Policy for Princeton University Information Technology
and Digital Resources

2015-2016 Edition

Policy Statement

The Acceptable Use Policy for Princeton University Information Technology and Digital Resources governs all uses of the University’s information technology resources whether administered by the Office of Information Technology or by individual departments. As stated in Rights, Rules, Responsibilities (RRR) members of the University community are expected to be familiar with and adhere to these policies.

Introduction to Policy on Acceptable Use of Princeton University IT and Digital Resources

The Acceptable Use Policy for Princeton University Information Technology and Digital Resources (this “Policy”) governs all use of Princeton University information technology, digital resources, and Internet access. Departments, programs 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 information technology resources and the access provided by the University to global networks and networked and digital resources are governed by the general policies and rules set forth in 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, including, but not limited to, websites, message boards, tweets, wikis, chat rooms, social networks, media-sharing sites, and other similar electronic venues; when they involve participation in MOOCs or virtual reality or gaming environments, or whether the technology involved is something like multi-user gaming, University-provided voice technology such as telephony Unified Messaging, locally-produced and broadcast video, or YouTube or other public arena videos or images involving University activities or operations. Individuals also are expected to be familiar with and comply with the requirements of the University’s Information Security Policy (www.princeton.edu/oit/it-policies/it-security-policy).
Reasons for this Policy
Some rules for appropriate use of the University's information technology resources derive from legal considerations. For example, the University must ensure that its non-profit status is not compromised by inappropriate political campaign or commercial activity. The University must also address actions that may violate its agreements with outside vendors. Additionally, these rules are intended to ensure that University resources and spaces are used to advance the University’s mission of teaching and research, while enhancing and embracing our diverse community.

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, materials or communications that individuals may post, send, or publish via the World Wide Web, Internet discussion groups, Facebook, YouTube, or any social networks; make available via any file-sharing method; or send via e-mail, tweeting, instant messaging or video; or any actions taken by individuals’ avatars within on-line virtual reality or gaming environments. However, under certain circumstances, the University may be required to respond to complaints regarding the nature or substance of such materials or communications.

Examples
The examples presented in this Policy focus on matters related to information technology, 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 violate the principles set forth in Rights, Rules, Responsibilities and be subject to University sanction. It is important to use common sense and critical thinking in evaluating new situations.

Because 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 and the Council for the Princeton University Community (CPUC) are charged with the task of revising Rights, Rules, Responsibilities, and any changes made to RRR could affect the language of this Policy.

Who must comply? What penalties pertain?

Compliance
This Policy applies to University-owned devices and systems and to University-contracted systems and services, as well as privately-owned or publicly-provided devices using the University’s networks and resources. This Policy applies to technology administered within the University Internet domain by individual departments or members of the faculty or staff or by campus organizations, 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; 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 including in student eating clubs, but connecting remotely to the University's network services and under the aegis of the University's name. This Policy applies also to actions of visitors to the campus who avail themselves of the University's temporary visitor wireless network access service or eduroam access, and to those who register their computers and other devices through Conference and Event Services programs or through other offices, for use of the campus network.

Privately-owned computer systems or mobile devices, or those owned by University organizations or by collaborative research projects, when attached to, or connected via, the campus data network and/or other campus resources or University-contracted services, 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 secure remote access software 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 location from which the misconduct originated or the network or devices used. Consistent with 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 or University-contracted services, must comply with the University’s policies. When a member of the University community is found to be in violation of this Policy, 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-account user is in violation of the 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 information technologies or the Internet.
Appropriate use of Princeton University IT and digital resources

Institutional 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 unified messaging systems; and to the Internet. Your use of all information technology should be for purposes that are consistent with the non-profit educational mission and the policies of the University, and should comply with any applicable license agreement and terms of service. Members of the University community are prohibited from using University information technology and digital resources for commercial purposes. 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, including the Information Security 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. Exceptions sometimes may be made for purposes of academic research.

Personal use
Personal use of the University’s IT and digital resources, 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 prevent the employee from attending to and completing work effectively and efficiently, does not incur additional cost to the University, 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.

Ensuring Accessibility
If you develop or acquire information technology and/or digital hardware, software, or systems for the University for use by students, faculty, staff or the public, you must make efforts to ensure that the result will be accessible to all individuals, including those with disabilities. If a service or system is not accessible at time of acquisition, you must work with the vendor to ensure that accessibility enhancements will be provided over time. You must also consider which modifications can be made upon request by an individual seeking a reasonable accommodation.

University access; your right to privacy
The University’s right to access files
All contents in storage on University and University-contracted 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 and copy files and documents (including e-mail and voice messages) residing on University-owned equipment, systems, and in storage contracted by the University from outside enterprises. 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, networking and monitoring systems staff will investigate and protective restrictions may be applied until the condition has been rectified.

Some departments that maintain servers or internal networks may 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.

The University also provides some access to files and documents residing on University-owned equipment and systems (and/or transmitted via the University’s network services) to outside vendors who have been contracted with to provide technology services. The University contracts with such vendors contain firm provisions for security of information and for the privacy of members of the University community who may use those services.

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. For example, employees 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 and digitized voice messages) stored on an employee's account or workstation must be accessed, whether because of unexpected absence, death, or termination of employment, or other necessity, such files may be accessed by the employing department after consultation with the Office of Human Resources, Office of Dean of the Faculty, Office of Dean for Research, and/or Department of Public Safety, as appropriate and based on business need. 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, and that copies of critical work product remain available following the employee’s separation from the University.

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 or message. The supervisor or designee 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. See University Records Management at 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 the Office of the General Counsel, including after an employee’s departure from the University.

Disclosure
In addition to information you may store on devices owned by the University, the University and its contractors maintain 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. Contact the Office of the General Counsel prior to disclosing any information in response to any subpoenas, court orders or other information requests from private litigants and government agencies.

Supervisors are encouraged to communicate the University’s expectations 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
Faculty and staff, including those who are designated as regular, term, visiting, and temporary, as well as student 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’s Record Retention Policy offers recommended retention periods for common University records whether on paper or electronic. Employees with questions should refer to the list of those with authority over specific sets of University information (www.princeton.edu/dataauthority) and/or to the University Records Manager.

Members of the University community, and especially employees, should understand that electronic information is governed by the same laws and regulations as paper documents historically have been, including statutes protecting the privacy of student records, medical information, and other kinds of personal information. Employees and students are expected to apply to electronic information the same security and record retention practices applied to paper documents.

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 needs to be shared, the greater the need to remove it from the e-mail system and store it as a hard copy (including the metadata accompanying the message, for example file properties or full e-mail headers) or in an electronic storage system. Attachments must also be identified and linked to the original message so that they may be easily located. In all cases, the authenticity and integrity of the entire e-mail message should be preserved.

E-mail retained in electronic format must be migrated by the account-holder to new software and storage media as upgrades occur.

Like all records, many e-mail messages eventually will cease to be useful to or needed by the department, and at that point should be deleted by the account-holder. Then the account-holder is responsible for assuring that the “Trash” or “Deleted Items” folder is emptied (either manually or on an automated schedule) to properly dispose of the e-mail records.

When a University employee trades in or replaces a computer or other networked device, it is required that the employee or the employee’s 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. 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 through approved University channels when no longer needed. However, it is imperative that copies of critical work
and work product be maintained until no longer needed. All discarding of media containing Princeton University information must be in compliance with the Information Security Policy.

Official e-mail
All members of the University community with ready access to e-mail are responsible for knowing the content of official correspondence sent to their University-provided e-mail address. Students who submit academic work via e-mail should retain copies of the work until certain that the instructor has received a legible copy. Acknowledgement by the instructor of receipt of a legible copy would be courteous and is encouraged.

Outside e-mail
Faculty, staff and students who have personal e-mail accounts with services outside the University should use only their University-provided e-mail accounts for communications regarding University matters. Using University e-mail protects the privacy and security of University data; allows for verification of sending and receipt of critical correspondence regarding academic and other matters; and facilitates 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 for their outside e-mail provider 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 other members of the University community.

Protecting data
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.

If you are a student and have information needed for completion of your University academics, you are responsible for assuring that adequate and appropriate back-up of the information is maintained.

Some kinds of information are considered restricted and/or confidential. Some information is protected by law, for example by FERPA or HIPAA. Some contractual agreements require protection of related information. Some research data, including data involving human subjects, must be kept confidential. In general, information should be protected consistent with the University’s Information Security Policy (http://www.princeton.edu/oit/it-policies/it-security-policy/).
As an employee or student, whether you have authorized or inadvertent access to what the University defines as restricted or confidential data, you must comply with the University's Information Security Policy and know which University office has authority over the information.

You also must confine your access to or viewing of such data to situations in which only your University responsibilities require such access or viewing.

Any handling of confidential 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, consistent with the Information Security Policy.

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 (www.princeton.edu/databreach).

If the individual suspects the breach involves illegal action by a member of the University community, the University's policy on reporting potentially illegal activity (www.princeton.edu/reportingillegalactivity) should be followed.

OIT's Help line (609-258-HELP by telephone, or helpdesk@princeton.edu via e-mail) is the best place to start when reporting potential data breach. If a related device is lost or stolen, a report should be filed as soon as possible with appropriate law enforcement. If the incident occurred off-campus, even outside the U.S., a copy of the relevant police report also should be obtained and provided to the Department of Public Safety.

Restricted or confidential data ordinarily should not be stored on mobile devices that are easy to carry away. If it is absolutely necessary to do so, the information must be encrypted to protect it from view should the device fall into unauthorized hands. The portable device and, ideally the files as well, must be password protected. It also is essential to provide adequate physical security for any device, including a desktop machine that contains confidential data.

Please note that if personal information from children under the age of 13 is collected for commercial purposes, such activities may be subject to the Children's Online Privacy Protection Act.

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. Information regarding encryption on University devices is published at www.princeton.edu/encryption.

Those who travel on University business or for study abroad should know that some encryption software may not be taken out of the United States. For that reason, and to avoid transporting
restricted or confidential data unnecessarily, 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. (For more information, see www.princeton.edu/itsecurity/intltravel.)

The advent of storage services in “the cloud” provides a useful alternative for those who use portable network devices or have computers stationary in several locations. The University has arrangements with certain providers for some secure cloud-based services. For example, faculty, staff, and graduate students may have Princeton-branded Google Drive accounts, which are subject to the Google Apps for Princeton University Usage Guidelines. (Undergraduate students have access to Princeton-branded Google Apps, which are subject to the Princeton and Google Terms of Service.) However, the security of cloud services not endorsed by the University still must stand the test of time. Until the University can endorse your doing so, storing confidential or private University information in other “cloud” services poses serious risks, and should be avoided.

Peer-to-peer file-sharing software may not be installed or used on DeSC computers (the set of machines designated explicitly for administrative applications) because such applications could expose to Internet access information that is restricted, confidential, or University-private. Other policies affecting DeSC computers may be seen at www.princeton.edu/descpolicy and at www.princeton.edu/descsecurity.

Protecting the University’s good name

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

Those who participate in social media as representatives or agents of the University should consult the Office of Communications’ social media policies (socialmedia.princeton.edu/guidelines) for guidance.

Use of the University's name and marks
As stated in RRR, "No individual or organization of the University may use Princeton University’s name, logos or other identifiers (“marks”), or any marks that suggest Princeton University or any other Princeton University organization, except to the extent such individual or organization has been authorized by the proper University authorities or as permitted under trademark law." Deliberate misuse of the name of the University or other marks by any member of the University community will be regarded as a serious offense.
The “people search” facility on the Princeton University home page returns a policy statement on acceptable use 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, and information available to the public must be consistent with the University’s policy on student information (RRR).

**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 to members of the University community 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.

**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 leave voice messages, 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 or general broadcast video materials, consider whether you would make those statements face to face with the person or people who may access your material. 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 personal characteristics or beliefs or their expression is subject to University disciplinary sanctions...."

**Harassment and defamation**

University IT and digital resources may not be used to transmit malicious, harassing or defamatory content.

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. Use of anonymity or pseudonymity in any form of electronic or digital 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, will be considered a serious transgression.

Technology has enabled ready and convenient use of recording instruments in ways not previously possible. Even unoccupied aerial vehicles allow access to areas once difficult or impossible to reach. Stand-alone or remotely-controlled cameras and other recording devices should not be used in places or ways that violate a reasonable expectation of privacy on the part of those whose activities are intentionally or accidentally 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 or 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 or the law. Departmental use of cameras or other recording devices on the campus, whether stand-alone or remotely-operated, is subject to the approval of the Security Advisory Group (SAG), by contacting the Department of Public Safety.

**Use of technology for commerce or solicitation**

**Commerce**

Members of the University community are prohibited from using University information technology and digital resources for commercial purposes. Campus-based organizations claiming national or regional status must use non-University IT or digital resources, including Internet access, for non-University 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 the University policy on accepting and handling credit and debit card payments, and other standards related to such e-commerce.

**Solicitation**

Electronic mail or World Wide Web, message board, social media, or Twitter solicitation using the University’s resources for fund-raising unauthorized by the University, even when conducted on behalf of non-profit organizations, 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. In some instances, a disclaimer of affiliation or endorsement may be advisable.

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. The University has contractual arrangements for those preferring outside hosting of departmental websites. If a different outside contractor maintains a website that you want to appear to be a Princeton University website, you typically will be required to obtain approval from the Office of the General Counsel.

If you maintain an outside website, other than through the University’s contractual arrangements, that you want to present or otherwise identify as a Princeton University website or affiliate, special authorization is needed. This often 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 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 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 and no substantial part of the University’s activities may be directed to influencing legislation.

A website is a form of communication. If something were to be posted on the University’s website that favored or opposed a candidate for public office or a political organization or solicited financial or other support for a candidate or a political organization, it likely 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 or a political organization. In addition, the University’s website may not be used to influence legislation.

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 or political activity or fundraising, or for influencing legislation. Faculty and staff also should refrain from use of University e-mail for campaign or political activity or fund-raising, or for influencing legislation.

Other political activity
Unless otherwise provided in RRR Section 1.5 or other University policy, University resources typically may not be used with respect to political activity. To the extent use is permitted, however, 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 typically acceptable. Questions regarding the use of University resources with respect to political activity may be directed to the Office of the General Counsel.

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 an account that provides access to the University’s 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, the University requires that passwords for University-provided accounts be changed at least once a year and for greater security recommends they be changed even 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.
A password used for access to a Princeton University account or resource should not be the same as those used to access non-University-affiliated resources. For example, account-holders should not use any of their University passwords as the password for a social media site, or a personal banking site, or other outside resources.

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 before the University recommends a secure option, you risk exposure and subsequent misuse of your University account access and files.

**Allowing access to others**
If you administer a server or router or allow accounts or access for others, whether members of the University community or people outside Princeton University on a networked device, system, server, router, or network address translator you own or control, you are responsible for protecting the University's property and good name from damage by others to whom you might provide access and for compliance by users with the University’s license agreements and any applicable terms of service. 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 (i.e., 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.

You also must be aware of and apply security updates and security patches as they are released for the software used to create and maintain the application and/or website.

Applications provided through cPanel or similar services on a University-maintained device will be scanned for vulnerabilities before being made operational, and any vulnerability should be
addressed. If serious vulnerabilities in such an application are observed after initial implementation, the website will be suspended 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 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 computer clusters managed centrally or by individual departments, 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, Webspace, SharePoint, Dormnet and access to 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 and there may be restrictions on the types of use permitted. 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 presently 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 such use is infrequent and the devices are not disruptive to network availability and performance. When possible, the eduroam service should be used as an alternative for infrequent wireless access. Temporary visitors with eduroam credentials from their home institutions are able with those credentials to use the University’s unrestricted campus services. Temporary visitors and members of the University community who use the visitor wireless service must comply with the University Policy regarding network and Internet use. Abusive behaviors that disrupt campus service can result in a device being blocked indefinitely from further use of any University network services.

**Mass mailings**

At Princeton, mass electronic mailings are permitted only as authorized by 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 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.

Those with disabilities requiring accommodation through specialized hardware, software, or other technology must have priority in the use of such items. If others are asked to cede access, they must do so.

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.

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 or toner cartridges 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. 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.

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

Computer procedures, programs, websites 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, even periodically, to interrupt or interfere with networked 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 possibly 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.

**Honesty, integrity, and the law**

The law
The University, including its faculty, staff and students, must comply with 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.

Members of the University community should report suspicion of crime involving, or revealed by, University technology resources (such as computers, mobile devices, network or Internet access, e-mail) consistent with the University's policy on reporting illegal activity (www.princeton.edu/reportingillegalactivity). For suspected crimes in progress or where there is an imminent or serious threat to individual safety, Department of Public Safety should be contacted immediately. In all cases, employees must treat information regarding potentially unlawful activity with discretion and sensitivity to the privacy rights of others.

Dishonest actions
There 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 using 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 account-affiliated resource or personal computer or networked device without authorization. If you encounter an open session that exposes another’s account-affiliated 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 message, 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 account-affiliated resources or another’s personal device or workstation, e-mail, or files, through deliberate action.

You must not attempt to fool others into revealing their log-in credentials or passwords, whether by use of social engineering, by tricking others into entering their credentials where key-loggers can capture the information, or by any other means. Log-in credentials (e.g., netIDs, user names and passwords) are highly confidential. To obtain another’s log-in credentials without that person’s knowledge and consent is unacceptable. Any attempt to capture another person’s log-in credentials is a serious offense and may be subject to disciplinary sanctions.

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, tablet, 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 evolving. 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 5.1.1 (www.princeton.edu/hr/policies/conditions/5.1/5.1.1/). This prohibition includes Internet gambling.

Gambling is a closely regulated activity in New Jersey. For further information regarding New Jersey’s position on Internet gambling, see the website for New Jersey’s Division of Gaming Enforcement (www.nj.gov/oag/ge/internetgaming_faqs.html).

Copyright and intellectual property

Copyright
The University’s policies concerning intellectual property are intended to further its central mission—the sustained production, preservation, and dissemination of knowledge—while exercising due care for its fiduciary responsibility for the resources it administers. The University and its community members are both holders and users of protected intellectual property. The University seeks to facilitate the responsible exchange of intellectual property and, to that end, works to raise awareness about issues of copyright, educating members of the community about principles of fair use, and providing resources to advance teaching and research.

Whether you are an author or a user of copyrighted materials, it is important to understand the legal context for copyrights. They are created by law and violations of the owner’s rights can be enforced through lawsuits. Even when the owner claims a violation has occurred, there are defenses and justifications for use of some copyrighted material. But it is crucial to start by considering whether the materials are protected by copyright – or not. Additional information about copyright can be found at the website provided by the Princeton University Library, the
Understanding copyright
“Copyright” is one name for a bundle of rights, including the right to make copies, distribute copies, making derivative works, and the public performance and/or public display of works. Copyright protects written works, paintings, sculptures, photographs, videos, recorded music, sheet music, computer programs, video games, architectural design, choreography, etc. Artists may also have moral rights to inclusion of the name of the artist on the work, and owners may have rights to prevent others from circumventing technological protections controlling access to the works.

Copyright does not protect every idea or scrap of paper. It does not protect ideas, concepts facts, data, titles, names, phrases, procedures or methods of operation. It also does not protect unoriginal works or works that are not fixed in a tangible medium (such as paper or digital code).

The creator is ordinarily the owner of a work, but owners can transfer some or all of the rights to a work. In general, under University policies, faculty and students retain the rights to their works. However, works created by staff in the context of their employment by Princeton are owned by the University. The owner can choose to allow certain uses by the public, and may even donate the work to the public domain.

Using copyrighted materials appropriately
Princeton encourages members of its community to make thoughtful, good-faith determinations that a use of copyrighted materials is a fair use in support of teaching and research, and to properly attribute those materials.

Fair Use is a flexible defense that allows socially valuable uses of copyrighted material, including educational copying. The “Fair Use” defense is intended to protect “transformative” uses of copyrighted works, primarily to create new art, literature, scholarship etc., without permission from the copyright holder. Information about how to apply the four fair use factors can be found at the University’s Copyright website ([www.princeton.edu/copyright](http://www.princeton.edu/copyright))

When doing academic work, you are responsible for properly attributing all material--data, images, ideas, sounds, film, and verbatim text--that you find through any sources, including the internet. 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.

Permissions
If you want to use a copyrighted work, you should make a good faith effort to determine whether such use constitutes a “fair use” under copyright law or seek permission of the copyright-holder. As a general matter, you are free to establish links to Web pages. But you are not generally free
to copy or redistribute the work of others publicly – even if you found it on the Internet – without authorization. Attribution does not resolve the issue of whether the use is permitted under copyright law.

Note that many creators do not themselves own their copyrights - the copyright in most books is effectively owned by the publisher; the copyright in most music is owned by a distributor. However, by contacting the creator you may be able to obtain permission (www.princeton.edu/copyright/getting-permission), or the creator may be able to put you in touch with the rights-holder. There are some collective licensing agencies that may be able to help you secure permission. The Library provides assistance in acquiring permissions for materials to be copied for library reserves, course materials, and other University-related purposes. Additional information is available about E-Reserves at library.princeton.edu/services/reserves/guidelines and also at www.princeton.edu/copyright. If your questions are not answered by University policies and websites, you can send an email to copyright@princeton.edu.

Members of the University community seeking permissions may not enter into agreements with vendors that would bind the University, unless the individual has proper authorization under the University Transaction Authority Policy.

Inappropriate use of copyrighted materials
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. Similarly, many software products are licensed for the campus community by OIT and may not be used elsewhere or by other users. Before using such licensed resources, you will be given notice of any relevant restrictions and are responsible for complying with them.

Your possession of copyrighted works – including music, video, games, etc. – does not necessarily bring with it permission to pass them on to others. You are responsible for determining the restrictions on music files, video files, podcasts, computer games, programs, packages, and data before copying them in any form or permitting them to be copied by others, using University resources. You may not circumvent copyright protection even on original media you own in order to make copies of the material.

There is an important distinction between accessing content through the channels the owner makes available, whether buying a DVD or through a Netflix subscription, and downloading additional copies of that content from the internet. Some people believe that, if they own a copy of a film or television show, they can then download a copy from the internet without infringing copyright. However, unless such copying has been authorized by the owner or for some reason qualifies as a “fair use” under copyright law, the downloaded file is an infringing copy.

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. Note that peer-to-peer file-sharing applications can establish shared space and share files without the intent or 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.

It also is a violation of copyright to allow unauthorized uploads of copyrighted material you may have downloaded legally, via Netflix or similar service.

Copyright enforcement by owners
The entertainment industry in the United States has become quite vigilant in pursuing people who infringe copyright. The recording industry has established a website at www.whymusicmatters.com regarding legal and illegal sharing of music, and the Motion Picture Association of America has established a website related to film, television, and copyright at 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. A comprehensive resource for legal sources of online content is maintained by the non-profit higher education organization Educause, and can be found at legal sources of online content.

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, administrative and support staff, and other 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. For example, people at the University have seen e-mail messages very cleverly designed to look as if they came from the Princeton Federal Credit Union. For tips on some of the dangers in Cyberspace, see the Information Security web page (www.princeton.edu/itsecurity). 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 story 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, Twitter, Instagram, 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 face of a Princeton residential college are generally protected from the immediate view of the general public, statements and images published, on the Internet can typically be seen anywhere, can last essentially forever, and can have serious unintended consequences.

“Thoughts on Facebook,” (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 Facebook 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 if 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 the General Counsel.

The University’s policy on reporting potentially illegal activity ([www.princeton.edu/reportingillegalactivity](http://www.princeton.edu/reportingillegalactivity)) describes procedures for reporting, including the third-party-managed Hotline for those who feel the circumstances warrant anonymity.

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 question 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

This section lists examples of acceptable behavior as well as behavior that may constitute a violation of University policy. The list is not all-inclusive; in addition, each situation must be considered in light of the specific facts and circumstances to determine if a violation has occurred.

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 do 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 Event Services 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 connected but unattended (or otherwise unprotected) in a common area of your dorm room or, if an employee, in your office or work space, 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, with identification of that 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.

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 legally obtained an 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 installer 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 commercial disk 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/Disruptive Behavior**

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 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, and create a sexually explicit message to 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 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.
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, tweet or IM to 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 send your posting only to the intended message board.

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 child has outgrown an infant stroller and you want to sell it. You use your University access to post a "for sale" notice to the relevant University message board. (Use of your University address in posting such a notice to an outside message board would not be appropriate under University policy.)

**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 online 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 record a debate between candidates for state office in order that a Politics class can view the video.

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 this 2015-2016 Policy

Representatives from the following groups and University offices participated in review and development of this 2015-2016 policy:

Graduate School Office
Graduate Student Government (GSG)
Institutional Equity and Diversity
McGraw Center for Teaching & Learning
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

Additional reading on related subjects

Go to the www.princeton.edu/itpolicy website, and click the “Additional reading” link within the left menu.