Acceptable Use Poe .

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   , judgments about such incidents will depend on the facts of an individual case.

- ## Penalties

All faculty, students, staü, departmental computer users, 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 mađer involves illegal action, law enforcement agencies may become involved, as they would for campus actions that do not involve information technologies or the Internet.

- ## Institutional Use

As a member of the University community, you are provided with scholarly and/or work-related tools, including (but not conýned to) access to the Library and its systems, to certain computer systems, servers, soĂware, printers, services, databases, and electronic publications; to the campus telephone and uniýed messaging systems; and to the Internet. Your use of all information technology should be for purposes that are consistent with the non-proýt educational mission and the policies of the University, and should comply with any applicable license agreement and term[illegible]
Universi[illegible] infoes any prety

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. By attaching privately ow eomBf s socty,d ily,i perf

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 (subject to any Legal Hold Notice issued by the Office of the General Counsel). See University Records Management at www.princeton.edu/records (http://www.princeton.edu/records). When 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.

Supervisors are encouraged to communicate the University's expectations regarding privacy of employee files and e-mail, and periodically to remind employees of these expectations. 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)

From time to time, members of the university community, including students, may use electronic means to collect data of interest to

When a University em

OIT's Help line (609-258-HELP by telephone, or helpdes @princeton.edu **(mailto:helpdesk@princeton.edu) via e-mail) is the best place to start when reporting potential data breach. (The phone line is staüed round the clock.) If a related device is lost or stolen, a report should be ýled as soon as possible with appropriate law Qat**

- 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.

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 to people or groups within the Princeton University community. The same principles that pertain to people or groups within the Princeton University community also apply to people or groups you may address outside the University community.

As stated in Rights, Rules, Responsibilities (https://rrr.princeton.edu/) ( ): "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 hostility 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 . Use of anonymity or pseudonymity in any form of electronic or digital communication for fraudulent purposes or with the intent to harass another, misrepresent oneself as another, or any other behavior in conflict with , will be considered a serious transgression.

Technology has enabled ready and convenient use of recording instruments in ways not previously possible. Stand-alone ent

University departments and groups that are authori

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.

Passwords are a significant method of protecting University systems against unauthorized use. Therefore 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, any password for a University-provided account that might have been exposed to capture must be changed at once, and to something different enough from the original to provide the necessary security.

Intentional sharing of 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.

The University now also protects certain services and resources via multi-factor authentication. Eventually, all University-provisioned accounts will be registered for such authentvleadurstec p andioyaled.eu d hrf tca,ulectcas ttp, eschyaṅ s iUÅV

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.pri

- Gambling

Gambling is prohibited for employees in the workplace except as speciýcally noted mpl

- Permissions

If you want to use a copyrighted work, you should make a good faith eüort to determine whether such use constitutes a “fair use” under copyright law or seek permission of the copyright-holder. As a general mađer, 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. Ađribution does not resolve the issue of whether the use is permiđed under copyright law.

Note that many creators do not themselves own their copyrights - the copyright in most books is eüectively 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/obt ining-permission **(hđp://www.princeton.edu/copyright/obtaining-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 about E-Reserves is avpso Reseishis dĎdiAw**

When creating public postings, twe

- Copyright, IP

Acceptable behavior: While browsing the World Wide Web, you ýnd 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 identiýcation of that page.

Acceptable behavior: You use a network sharing tool to download audio format music ýles for which you have obtained permission, or ýlesy telatsi oná esafg whiedtoy,rhat wbtaiAcdapŏmi sioow,ana yowpasdvcorp-protect those ýles so no one without authorization can get them from your device. en have a net hota sh a createeag terkuo u etact

Acceptable behavior: You-are testing a beta-release soĂware, and know it could ýx 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.

Violation: You have legally obtained an online copy of a ýlm or television show ýle. You have a network sharing tool empowered, which permits others around the world to upload copies of that ýle from your storage space,c You A res word-pele ck t ge) etoctor ou

Violation: You change the system sound on shared cluster or lab computers to

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- (