GUIDELINES FOR COMPLIANCE WITH THE TECHNOLOGY ACCEPTABLE USE POLICY

TABLE OF CONTENTS

OVERVIEW

These guidelines [i]are intended to help Our Lady of the Lake University (OLLU) students, faculty, staff, alumni, guests, and other affiliates better comply with the intent of the University's Technology Acceptable Use Policy (AUP).

OLLU's information technology resources and the access provided by the University to global networks and networked and digital resources are governed by University general policies and core values. The principles and expectations set forth in these documents 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, augmented reality, 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 Program.

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 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, Instagram, 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 these guidelines 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 as inappropriate, it still may violate the principles set forth in the student, faculty or employee handbooks and be subject to University scrutiny. 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, the Acceptable Use Policy will continue to evolve. Therefore, the examples provided will also evolve over time.

VIOLATIONS AND PENALTIES

All faculty, students, staff, alumni, 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 such policies, 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 is in violation of such policies, the University sponsor or host may be held accountable. If the matter involves illegal activities, law enforcement agencies may become involved, as they would for campus actions that do not involve information technologies or the Internet.

As described in the student, faculty and employee handbooks, violations of University-wide rules of conduct by members of the OLLU 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, employees, contractors, and guests. Violations by employees may result in disciplinary action including possible termination. Violations by students may result in suspension of network privileges or expulsion from the University. Violations of applicable state or federal laws by any party may result in civil or criminal prosecution.

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 limited 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; to mobile devices; 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 agreements 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 is no longer is needed, its disposition must be in compliance with University policies, including the Information Security Program, 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 agreements 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.

THE UNIVERSITY'S RIGHT TO ACCESS INFORMATION

All contents in storage on University and University-contracted data and voice systems are subject to the information monitoring rules of OLLU, 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.

Information Technology Services (ITS) may collect usage data and may monitor servers and networks to ensure adequate technical performance. ITS is 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 to provide technology services on behalf of the University. The University contracts with such vendors must contain firm provisions for security of information and for the privacy of members of the University community who may use those services.

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 Compliance Officer prior to disclosing any information in response to any subpoenas, court orders or other information requests from private litigants and government agencies.

RETAINING WORK-RELATED FILES

On employee termination, supervisors are expected to assure that passwords to computers, other networked devices, mobile devices, and information system 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.

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. Where the Compliance Officer has issued a "Legal Hold Notice," individuals may be required to suspend regular retention practices and to retain information until further notice from the Compliance Officer, 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 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 in electronic form. Employees with questions should contact the Office of the Vice President for Administration.

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 data export or record-keeping system, for example, Outlook archive files. 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 format. 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 data custodian 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 data custodian. Then the data custodian 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 computer or other networked device is being refurbished or decommissioned, it is required that the device's storage systems have any and all data securely removed from the hard drive or, if that is not possible, to destroy the storage device 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 OLLU information must be in compliance with the Information Security Program.

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.

OLLU account-holders who have their e-mail copied or forwarded to an outside account must take care to avoid having these messages flagged as spam by their outside email service provider. Major Internet service providers potentially could bar all e-mail coming out from the OLLU domain when the provider's customers have marked as spam what the provider perceives to be as too many suspicious 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 Program.

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 Program 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 devices, should be done in the most secure, confidential manner, consistent with the Information Security Program.

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.

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 should be followed.

ITS’s help line (210-431-3908 by telephone or helpdesk@ollusa.edu via e-mail) is the best place to start when reporting a 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 University Police.

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 protected with a PIN or passphrase. 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 device you use, you should be prepared to use one when it is announced as endorsed. Information regarding encryption on University devices is provided within the University’s Information Security Program.

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 OLLU.

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 students have access to OLLU-branded Microsoft Office 365 OneDrive and Team accounts. 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 OLLU computers without written authorization from the Information Security Officer because such applications could expose to Internet access information that is restricted, confidential, or University-private.

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 OLLU 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 Marketing and Communications social media policies for additional guidance.

USE OF THE UNIVERSITY'S NAME AND MARKS

No individual or organization of the University may use OLLU's name, logos or other identifiers ("marks"), or any marks that suggest OLLU or any OLLU organization, except to the extent that 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.

DIRECTORY USE

Information in OLLU's on-line campus directories are provided solely for use by members of the OLLU 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.

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 OLLU community as to those within.

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 reasonable care to ensure that inappropriate images, sounds or messages which could create an atmosphere of menace or harassment for others are not displayed on workstations in these locations.

You also must refrain from transmitting to others in any location inappropriate images, sounds or messages that are clearly threatening, hostile, or harassing. Use of anonymity or pseudonymity in any form of electronic or digital communication for fraudulent purposes or accomplished with the intent to harass another, misrepresent oneself as another, or any other behavior in conflict with OLLU's core values will be considered a serious transgression.

Technology has enabled ready and convenient use of recording instruments in ways not previously possible. Today, unoccupied aerial vehicles (a.k.a. drones) can enable video recording of areas once considered extremely 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 video recording devices on the campus, whether stand-alone or remotely-operated, is subject to the approval of [what should go here?].

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 phone, over the campus network, or over the Internet must comply with the University Information Security Program 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 an OLLU web page, care must be taken not to do so in a manner that suggests the commercial site has the endorsement or support of the University unless that has been authorized by 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 an OLLU web page, you must do so in a manner that will not suggest the University sponsors, endorses, or otherwise supports the outside site.

If you maintain an outside website, other than through the University's contractual arrangements, that you want to present or otherwise identify as an OLLU website or affiliate, special authorization is needed. This often requires review by the Office of Marketing and Communication and the Compliance Officer. The same is true if you want to create a website internal to OLLU 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 general University policies permit otherwise, 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 Vice President of Administration.

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 alumni, 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, to keep them strictly confidential, and to safeguard them from casual observation or capture. Thereafter, the University requires that passwords for University-provided accounts be changed at least once every 90 days and for greater security recommends they be changed even more often.

In addition to regular password changes, university-provided accounts must be regularly used and monitored. All account holders are expected to regularly exercise the use of their OLLU accounts multiple times during the year by logging into and using the services we provide to you. For example, all account holders are expected to actively monitor their OLLU email accounts by logging into Office 365 periodically or by logging into a campus computer and opening Outlook; if you are a student, we expect that you will be regularly logging into your Blackboard account to check for updates; etc. Any account that is not regularly exercised in this way during the course of a year may be deactivated for inactivity.

Intentional sharing of account 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 an OLLU 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.

For each account provided by the University to you, a different password should be used. The same password should not be used for different OLLU systems.

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 administer accounts or access for others, whether members of the University community or people outside OLLU 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 should not administer access for others. You are responsible for assuring that a strong root or administrative password is in place; for ensuring operating systems are updated promptly; 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 OLLU domain, or for other hostile or abusive purposes.

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 on a University-maintained or network connected device must be scanned for vulnerabilities before being made operational, and any vulnerability should be addressed. If serious vulnerabilities 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 OLLU Help Desk, the Library Office, the Information Security Officer, the Chief Technology Officer, or the appropriate system authority, either within or outside the University. 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 ITS or the University Library, 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, 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, SharePoint, OLLU's email 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 meet the demand, certain performance-related or sharing guidelines pertain.

ITS 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 improperly 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 provided 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 OLLU participant's devices 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.

MASS MAILINGS

At OLLU, 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.

"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 recipients 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 using 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 needs for software and services available in only one location, and cede access 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 that you wish to continue using 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 processes running on that device may be terminated.

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 efficient and cost-effective printing. When a work is in progress, editing should take place on-line whenever possible rather than on a printed draft. Preference should be given to sharing information electronically rather than in printed form as much as possible. 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 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 packet capture systems, "sniffers" (programs used to capture information being transmitted) on any portion of the campus wired or wireless networks without authorization. You may not operate Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BootP) servers on the campus networks without authorization.

You must not attempt to obtain system privileges to which you are not entitled, whether on OLLU 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 the 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.

Wireless access points or other devices such as printers with wireless access point capabilities may not be installed/enabled by individuals in campus academic, administrative, or service buildings, including buildings rented or owned by the University off campus, without authorization from the ITS. If authorization is provided, the individual must comply with any rules regarding the wireless access point established.

Computers, smart phones, and other network devices connected to the University's network are 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 assigning another IP address for use in any network transaction.

UNDER 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 crimes 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. For suspected crimes in progress or where there is an imminent or serious threat to individual safety, University Police 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 or unethical and are contrary to OLLU's core values of integrity and trust. Such actions also are unacceptable when conducted by means of the University information technology resources and Internet access. Deliberate violations will be considered serious offenses; subsequent violations, or systematic violations in the first instance, will be considered extremely serious.

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 without authorization.

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 OLLU 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 OLLUSA.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., 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 is no longer meaningful.

You may not "borrow" an Internet Protocol address assigned to another person or entity, create a fraudulent IP address for a device you own or are using, or attempt to use on one device the IP address assigned to another. 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 OLLU's network.

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. This prohibition includes Internet gambling.

COPYRIGHT AND INTELLECTUAL PROPERTY

COPYRIGHT

The University's policies concerning intellectual property are intended to further its central mission 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 OLLU Library.

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 OLLU 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

OLLU 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. For more information about how to apply the four fair use factors, please contact the OLLU Library.

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 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 the 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, 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.

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.

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 ITS or other departments and may not be used elsewhere or by other users.

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 a 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.

COPYRIGHT VIOLATIONS AND PENALTIES

UNIVERSITY PENALTIES

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 the Student Handbook.

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 tips on some of the dangers in Cyberspace, see the StaySafeOnline.org website. 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 ITS at OLLU or at some financial institution and ask the person for his or her account login 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. Communications, photos, videos, and other postings in online social media sites like Facebook, Instagram and Twitter may be seen anywhere, can remain accessible on the Internet for decades, and can have serious unintended consequences.

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 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, Office of Human Resources, University Health Services, Information Technology Services, Office of the VP of Administration, and University Compliance Officer.

The University’s policy on reporting potentially illegal activity describes procedures for reporting, including the third-party-managed Hotline for those who feel the circumstances warrant anonymity.

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 OLLU'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 an OLLUSA.EDU domain return address.

Acceptable behavior: A group of visiting scholars has arranged through Conference and Event Services to have University wireless network access and account IDs during their stay on campus.

Violation: You have a departmental computer account that provides access to certain shared files, to OLLU'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 ollusa.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 you downloaded via a legal service such as iTunes, and you want to use it as a kind of personal theme song. 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: 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 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 others in the OLLU community 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 computing 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 an upcoming event.

Acceptable behavior: Someone "spams" you; you refrain from replying, 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 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 a community message board. (Use of your University email 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 OLLU and use e-mail to communicate with potential employers.

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

Acceptable behavior: Your recognized student organization has a CD that the group has been authorized to sell via the World Wide Web. You offer it for sale following the regulations for e-commerce established by the Finance 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 webserver page explaining its activities. Rather than just stating 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 OLLU."

Violation: You are a University employee who manages a summer camp for children interested in chess that is not affiliated with OLLU. You use your OLLU e-mail address and affiliation to advertise the camp.

Violation: You run an advertisement of your own for-pay service on your university-provided user 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 OLLU supports a current candidate for political office.

ADDITIONAL READING

RELATED OLLU DOCUMENTS

- Technology Acceptable Use Policy – http://aup.ollusa.edu
- Information Security Program
- Record Retention Policy
- Social Media Policy
- Mobile Device Policy
- Student Handbook
- Faculty Handbook
- Employee Handbook

ENTERTAINMENT INDUSTRY SITES

- Motion Picture Association of America site on respecting copyright
- Music industry site on music file-sharing
- Industry information on campus downloading
- Music, Movies and Computer Software Copyrights
- ESA Entertainment Software Association

LEGAL ALTERNATIVES FOR DOWNLOADING

- EDUCAUSE list - legal sources of copyrighted material
- Legal sources of films and TV shows

SPECIAL ORGANIZATIONS, TASK FORCES, AND SPECIAL REPORTS

- The American Civil Liberties Union
- Collection of fair use documents/sites/reports and the result of the national conference on fair use
- Copyright Clearance Center FAQ
- The Electronic Frontier Foundation (free speech organization)
- New Jersey Division of Gaming Enforcement

- FIRE - Foundation for Individual Rights in Education
- PEACEFIRE - Teen Net Anti-Censorship Alliance
- US Copyright Office homepage
- US Department of Justice Computer Crime and Intellectual Property Section

[i] OLLU gratefully acknowledges the permission to use content and structure from Princeton University to develop these guidelines.