Yeshiva University Staff
Technology Resources Use Handbook

Introduction

Yeshiva University ("**YU**" or the "**University**") provides various technologies, including computers, Internet access, email, and telephones (including smartphones), to its staff to facilitate the exchange of ideas and information, and to aid in the University's communications and work-related research. In addition, these technologies are provided to staff so that they will have maximum access to resources and information they need to perform their assigned duties. These technologies are provided for legitimate business use in the course of a staff member's completing assigned duties. The following policies are intended to clarify the range of permitted uses of the University's technologies.

It is important for all staff members to read and understand this Handbook and the policies contained herein. Policy violations may have serious consequences.

The University reserves the right to revise and modify the policies contained in this Handbook in its sole discretion. Nothing in this Handbook creates any expectation of privacy or alters any employment relationship. Questions concerning this Handbook and the policies contained herein should be addressed to the University's Information Security Administrator at infosec@yu.edu. Any misuse of University computers or computing resources, or evidence of intrusions or tampering, should be promptly reported by email to abuse@yu.edu or abuse@einstein.yu.edu.

As a condition of a continued working relationship with the University, each staff member must:

- read and comply with all University policies, including those contained in this Handbook; and

- annually sign a form acknowledging that he or she has received a copy of this Handbook and agreeing to comply with the policies contained herein. Any University staff member with access to the University's Information or Technology Resources must comply with the University's policies and procedures relating to information security.

All information stored, transmitted or handled by the University's Information or Technology Resources is the property of the University. Subject to applicable law, University personnel may review and monitor this information at any time without employee permission for administrative, security and other lawful purposes.

Definitions

Confidential Information: any information relating to the University's operations that, if disclosed to an unauthorized individual or entity, could result in substantial harm to the University. Confidential Information includes, but is not limited to, student information

(including financial, financial aid information and grades); business projections; business/academic plans; proprietary processes; research information; compensation information; job performance ratings or appraisals; tenure files; pending sales, purchases or contracts; patient and research participant information; and fundraising and development information.

Copyright: legal protection for original works of authorship that are fixed in a tangible means of expression. Text (including email and web information), graphics, art, photographs, music, film and software are examples of types of work that may be protected by copyright.

Document: any letter, memorandum, tape recording, electronic mail, electronic document, note, or written communication.

Highly Sensitive Information: a subset of Confidential Information and Personal Information that has special sensitivity including an individual's name in combination with: (i) Social Security number, passport number or other government identification number; (ii) driver's license number; or (iii) financial account number, such as a credit card or debit card number, with or without any code or password that would permit access to the account; or (iv) medical or health information, such as disability information, treatment history and health insurance information.

Incidental Personal Use: occasional, non-commercial personal use that takes place outside of normal work hours at negligible cost to the University and does not interfere with the University's needs or operations or a staff member's job.

ITS: the Information Technology Services Department.

Network Administrator: the person(s) responsible for managing telecommunications network software, hardware infrastructure, or access rights for local area networks (LANS) or wide area networks (WANS).

Peer-to-Peer (P2P): software, services, and protocols that are commonly referred to as "peer-to-peer" or "P2P," including applications such as, but not limited to, BitTorrent, LimeWire, Gnutella, Kazaa, IMesh, and Bearshare. P2P includes, without limitation, software that enables the sharing of files among a network of computers without a need for centralized storage of such files.

Personal Information: information that can be used to identify any individual. Personal Information includes an individual's name, work or home address, email address, telephone or facsimile number, Social Security number ("**SSN**") or other government identification number, employment information and background information, financial information, medical or health information, such as an individual's health insurance identification number or condition, account numbers, certificate or license numbers, vehicle identifiers and serial numbers (including license plate numbers), device identifiers and serial numbers, biometric identifiers (including finger and voice prints), and photographs. Personal Information may relate to any individual, including

University students, faculty, staff, officers, directors, consultants and individuals associated with students, faculty, staff, consultants, vendors and other third parties.

System Administrator: the person(s) responsible for managing central computer or file servers, including operating systems and application software.

Technology Resources: consists of all University-owned personal computers and workstations, including notebook computers; mini and mainframe computers and associated hardware such as disk drives and tape drives; peripheral equipment such as printers, modems, fax machines, copiers, telephone equipment; personal devices such as BlackBerry devices, other PDAs and cellular phones; computer software applications and associated files and data; remote access to the University's network; and access to outside sources of information such as the Internet.

University community: refers to all University administration, staff, faculty and students.

User(s): all University staff members with access to Technology Resources.

Yeshiva University Information: any information that is collected, used or maintained by the University. Yeshiva University Information may include any Confidential Information or Personal Information (including Highly Sensitive Information).

Using Technology Resources

All Technology Resources under the control of YU are provided for the furtherance of the University's academic and business pursuits. YU extends access privileges to members of the University community and expects them to comply with all applicable University policies and applicable state and federal laws in accessing these resources.

No User may use the Technology Resources for the conduct of non-University business, including private solicitations.

Notwithstanding the above, Users may use the Technology Resources for Incidental Personal Use. Examples of Incidental Personal Use include using the Technology Resources to:

- prepare and store incidental personal data (such as personal calendars, personal address lists, personal email, personal Internet links and similar incidental personal data) in a reasonable manner, provided such use does not conflict with any purpose or need of the University.

- send and receive necessary personal communications through email.

- use computers and BlackBerrys to conduct personal transactions and retrieve information of personal interest from the Internet, provided such activity excludes

prohibited activity (listed in the Internet Access and Use Policy) and is brief and in balance with authorized or reasonable break periods.

- use the telephone system for brief and necessary personal calls.
- participate in University-sponsored Internet communities within defined guidelines.

The following are examples that do not qualify as Incidental Personal Use and are not appropriate unless required for the User's position at the University:

- viewing, sending or drafting gross, indecent or sexually-oriented materials.
- visiting gambling sites.
- visiting illegal drug-oriented sites.

Using the Technology Resources to commit illegal acts or harass an individual or organization is not considered Incidental Personal Use.

The University assumes no liability for loss, damage, destruction, alteration, disclosure or misuse of any personal data or communications transmitted over or stored on the Technology Resources. YU accepts no responsibility or liability for the loss or non-delivery of any personal email communication. The University reserves the right to suspend or limit privileges as required in its sole discretion to protect and operate the Technology Resources.

Privacy

User Privacy

Subject to applicable law, all information created, sent, or received via the Technology Resources may be reviewed and monitored by University personnel at any time for any reason without employee permission.

Users do not have a personal privacy right in any material created, received, saved or sent by the Technology Resources. The granting of a password does not confer any right of privacy upon any User. Users should assume that all documents created or saved on the Technology Resources are the University's property.

Users who use the Technology Resources to create or maintain personal information or messages have no right of privacy with respect to those messages or information. The University provides the Technology Resources only to further its own academic and business aims. All Technology Resources and all information, documents and messages stored on the Technology Resources should be related to the business of the University (except as noted in this Handbook).

The best way to guarantee the privacy of personal information is not to store or transmit it on the Technology Resources.

Yeshiva University Privacy

The University seeks to ensure that information and messages stored and transported on the Technology Resources are safe from unauthorized use or examination. Users should not, however, assume that information or messages stored or transported on the Technology Resources are safe from unauthorized access. Users should comply with the Related Policies listed below in order to enhance the privacy of student and University information:

Related Policies in this Handbook:
Information Security & Technology Resources
Internet Access and Use
Electronic Mail (Email)

Installation and Use of Software

The loading and unloading of any software package onto or off of a University-owned system must be properly licensed and compatible with the University's network. It is the University's policy that all software in use on the Technology Resources is officially licensed to YU. The staff member loading onto, or otherwise utilizing software on, the Technology Resources is responsible for ensuring that the software is properly licensed. Further, all software purchased by, licensed by, or created by the University is the exclusive property of the University. Without the prior written authorization of an authorized representative of ITS, Users may not:

- install University-owned or licensed software on any non-University-owned computer equipment; or

- provide copies of University-owned or licensed software to anyone.

Related Policies in this Handbook:
Use of Copyrighted Material
P2P File-Sharing Policy

Use of Copyrighted Material

All members of the University community are responsible for complying with copyright laws (and other intellectual property and proprietary rights). In general, copyright laws protect and grant exclusive rights to authors of published or unpublished original works that have been recorded in tangible form, including literary works, musical works, dramatic works, pantomimes and choreographic works, pictorial, graphic, and sculptural

works, motion pictures and other audiovisual works, sound recordings and architectural works.

In compliance with copyright laws and this Handbook, Users may not:

- copy, distribute, download or upload copyrighted material to and from the Internet in a manner that violates the owner's copyright protections;

- copy, distribute, download or upload copyrighted material from original media in a manner that violates the owner's copyright protections; or

- use P2P file-sharing software on the University's network except as authorized by ITS in writing.

With the cooperation of all Users, an authorized representative of ITS shall be responsible to ensure that all copyrighted material found or utilized on the University's machines is properly licensed. For more information on the University's policies regarding copyrights, please see the Yeshiva University Digital Millennium Copyright Act (DMCA) policy on the University's website and also available from ITS. A User's unauthorized distribution of copyrighted material, including P2P file-sharing, may subject the User to civil or criminal liability.

Related Policies in this Handbook:
Installation and Use of Software
P2P File-Sharing Policy
Internet Access and Use

P2P File-Sharing Policy

ITS is responsible for the design, throughput, availability, and overall health of the University's network. Peer-to-Peer (P2P) file-sharing software is used to connect computers directly to other computers in order to transfer files between the systems directly, without the need for centralized storage of those files (for example, on centralized servers). Frequently, this software is used for the transfer of copyrighted materials such as music and movies. ITS generally does not monitor the identities of the specific data or files that Users download or copy over the University network. ITS does, however, monitor and study specific types of network traffic and the applications that generate this traffic. P2P software, when abused, can saturate an entire network and leave some or all of its users with poor to non-existent performance. Additionally, the use of P2P software needs to be restricted in order to comply with the letter and intent of the Yeshiva University Digital Millennium Copyright Act (DMCA) policy.

In order to prevent any type of abuse (whether accidental or intentional), no P2P software may be used on or in connection with the Technology Resources, and the Technology Resources may not be used for any type of P2P file-sharing or similar

activities. Exceptions can be made only with the express prior authorization of ITS, in ITS' discretion (see below).

Possible Exceptions—Authorization for Use of P2P Software

As noted above, exceptions for specific uses of P2P software may be made for specific Users (for example, if a User's work requires the use of a specific item of P2P software). Such exceptions may be made by ITS in its sole discretion. A request for such an exception may be made by submitting a Support Request Form or by contacting the ITS Help Desk. As an example, a P2P application such as BitTorrent may have specific value for a particular type of work, such as the exchange of scientific information in connection with a particular project, and therefore a particular User may request that an exception be made.

- ITS reserves the right, in its sole discretion, to authorize use of P2P software on a per-User, case-by-case basis, when provided with specific, written purposes directly related to, or in support of, the academic, research or administrative activities of the University.
- Permission to use P2P software may be revoked at the discretion of ITS. This includes, but is not limited to, revocation for one or more of the following reasons: service abuse; degradation of the performance of the University network; and use for purposes other than University business or the specific purposes for which the exception was granted.
- ITS reserves the right to periodically review Users' use of P2P software and activities that have been permitted pursuant to such exceptions.

User Responsibility

- Users must educate themselves on P2P software through the resources provided on the ITS website.
- Users must not knowingly download, install, or use P2P software without ITS' authorization. This includes a User configuring any resource attached to the YU network (including his or her computer) so that files stored on or in connection with such resource are available to other Users or third parties using P2P software or protocols.
- Users must remove any P2P software that is discovered on any resource attached to the YU network, including personal property, unless granted specific permission by ITS in advance.

Enforcement of P2P Policies

To prevent the use of P2P applications, ITS blocks well-known "ports" that are used by P2P software and protocols; however, some P2P applications are still able to negotiate

connections on other, dynamic ports. If ITS detects a system engaging in P2P activity, ITS reserves the right to block all such activity and/or to disconnect such system. Continued unauthorized use of P2P software over YU's network may result in disciplinary action or termination of access.

Related Policies in this Handbook:
Installation and Use of Software
Use of Copyrighted Material
Internet Access and Use

Information Security & Technology Resources

All members of the University community must properly safeguard and handle Yeshiva University Information, regardless of its form (*e.g.*, electronic records) as more fully set forth below. Users are responsible for preventing unauthorized access to, and protecting the security and confidentiality of, Yeshiva University Information.

Authorized Access

Users may not allow any person to access, in any manner, their assigned computer equipment unless that person is specifically authorized to access such equipment. Users should not disclose their passwords to anyone. A common method for hackers to gain access to computer networks is for the hacker to impersonate a member of ITS. The hacker will call a User with a story that he or she needs the user's login ID and password. Members of ITS will never call a User and ask for a login ID and password.

The fact that information stored on the Technology Resources is *accessible* does not necessarily mean that access to it is *authorized*. Even when physically able to, Users may not access any information other than that which they are specifically authorized to and which is necessary for the performance of their assigned duties.

Data Retention

It is recommended that each User take such action as he or she deems reasonably appropriate to ensure that his or her computer files are properly backed up. All costs and expenses so incurred shall be subject to customary University approval.

For more information, please see the Yeshiva University Employee Handbook or contact the ITS Help Desk by calling #6123 from campus phones or (212) 960-5294 from non-campus phones or by email at helpdesk@yu.edu for data backup storage and archival solutions.

Please be aware that the use of "cloud computing services", such iCloud, Dropbox, Microsoft (Azure, BPOS and SPLA), Amazon (AWS, S3 and EC2) and Google (Google Apps) may create potential security breaches. It is recommended that such services should not be used without first consulting with an authorized representative of ITS.

Related Policies in this Handbook:
Protection of Confidential Information and Personal Information
Password Policy

See also the Yeshiva University Employee Handbook and Yeshiva University Record Retention Policy

Protection of Confidential Information and Personal Information

YU is dedicated to protecting the security and confidentiality of the Confidential Information and Personal Information that it collects, uses and maintains. While working at the University, Users may create, discover, use, access, receive or otherwise handle Confidential Information and Personal Information. No matter what a User's position or role at the University, every User has an obligation to safeguard Confidential Information and Personal Information. Please see the Yeshiva University Employee Handbook for more information.

All University staff members must properly handle the Confidential Information and Personal Information that they collect, use or maintain in the course of business. Accordingly, Users have an obligation to safeguard Confidential Information and Personal Information in electronic form. This obligation includes:

- preventing unauthorized access to, and protecting the security and confidentiality of, Confidential Information and Personal Information in electronic form;

- only collecting, accessing, using, maintaining, transporting or disclosing the minimum amount of electronic records containing Confidential Information and Personal Information that is necessary and relevant to perform the User's job responsibilities;

- only removing electronic records containing Confidential Information and Personal Information from the University's offices when it is necessary and relevant to perform job responsibilities;

- not using electronic records containing Confidential Information and/or Personal Information for unauthorized purposes and not permitting them to be used for unauthorized purposes;

- properly disposing of electronic records containing Confidential Information and/or Personal Information in a manner that is commensurate with the degree of risk posed by any disclosure of such information (*e.g.*, ensuring that SSNs are disposed of so as to make them unreadable, such as by wiping or shredding electronic media that contain SSNs); and

- notifying abuse@yu.edu if a User believes electronic records containing Confidential Information and/or Personal Information has been obtained or accessed by an unauthorized person.

Each User's obligation to safeguard electronic records containing Confidential Information and Personal Information extends to all situations in which a User may handle such information, including when the User is away from work or working remotely.

In general, Highly Sensitive Information should not be stored on portable or removable devices, including laptops, unencrypted USB drives, unencrypted removable drives or portable media (*e.g.*, CDs and DVDs). If there is a business purpose to store Highly Sensitive Information on portable or removable devices, the Highly Sensitive Information must be encrypted. Confidential Information and Personal Information should not be stored using public Internet storage, including "cloud computing services", such iCloud, Dropbox, Microsoft (Azure, BPOS and SPLA), Amazon (AWS, S3 and EC2) and Google (Google Apps). Users should consult with an authorized representative of ITS and the Office of the General Counsel if they require an exception to this rule.

Highly Sensitive Information may not be transmitted, by any means, to persons outside of YU unless all of the following conditions are met:

1) The Highly Sensitive Information is encrypted in a computer file or stored on an encrypted device;

2) The transmittal text includes a warning to the recipient that the material contains Highly Sensitive Information and is the property of YU; and

3) The transmittal text contains a specific statement of why the recipient is receiving it, what he or she may do with the information, and to whom, if anyone, he or she may disclose it.

Confidential Information may not be transmitted, by any means, to persons outside of YU unless the following conditions are met

1) The Confidential Information is password protected in a computer file; and

2) The transmittal text includes a warning to the recipient that the material contains Confidential Information and is the property of YU.

All Users must ensure that any Confidential Information or Personal Information will only be taken out of YU's facilities for allowable business purposes and will be encrypted.

Related Policies in this Handbook:
Encryption Policy
Technology Resources Disposal
Remote Access
Work Outside of Yeshiva University's Premises
Laptops and Other Portable Devices

See also the Yeshiva University Employee Handbook

Physical Security of Technology Resources

Users must ensure that all Technology Resources (computers, monitors, laptop computers, printers, phones, etc.) that are assigned to or regularly used by them are maintained and used by them in a manner consistent with their function and such that the possibility of damage and/or loss is minimized.

Computer equipment (other than laptops and other portable data equipment supplied by the University for a User's use outside of the University's premises) belonging to the University or maintained by ITS may not be removed from the University's premises without the prior written authorization of an authorized representative of ITS. Without the prior written authorization of an authorized representative of ITS, Users may not modify the University's computer equipment in any manner including, but not limited to, attaching external disk drives, external hard drives, changing the amount of memory in the computer, and attaching/installing any peripheral device, including wireless routers. ITS will authorize all User modification that may be necessary for business purposes. This section shall not apply to ITS personnel while performing their assigned duties.

All of the Technology Resources must be:

- located in physically secure locations appropriate to the sensitivity of the resource; and
- placed in controlled and protected environments such that their purpose, functionality or effectiveness is not placed in jeopardy, including, for example:
    - placing file servers and routers outside of YU's general computer centers in locked closets;
    - physically securing all laptops to desks with cables; and
    - storing all master copies of software in secure containers.

Related Policies in this Handbook:
Technology Resources Disposal
Laptops and Portable Devices

Electronic Access Controls

Except with prior authorization from ITS, a User may not:

- test or attempt to compromise internal and preventive controls of any Technology Resource, such as system configuration files or antivirus parameters; or
- exploit vulnerabilities in the security of any Technology Resource for any reason, including, but not limited to:

- damaging systems or information;
- obtaining resources beyond those he or she has been authorized to obtain;
- taking resources away from other Users; or
- gaining access to Technology Resources for which proper authorization has not been granted.

All University-owned computers should have personal firewall software installed. This software is to remain activated and set to the highest protection status possible that supports business purposes at all times. An authorized representative of ITS will ensure that the software is updated as appropriate.

For systems and devices under ITS' ownership or control, ITS will ensure that all security updates for operating systems, web browsers, server applications, and email clients are installed in a timely manner.

For systems and devices that are not under ITS' ownership or control but are authorized to process YU's data and/or attached to the YU network, the User must ensure that all security updates for operating systems, web browsers, server applications, and email clients are installed in a timely manner.

Related Policies in this Handbook:
Password Policy
Encryption Policy
Anti-Virus Protection

Password Policy

Users must comply with all applicable guidelines promulgated from time to time by ITS (including, without limitation, the length of the password) in selecting passwords. In accordance with industry standards, Users must choose passwords that cannot be easily guessed. In addition, passwords should not be related to a User's job or personal life. For example, a car license plate number, a spouse's name or an address should not be used. Moreover, passwords also should not be words found in the dictionary, and proper names, places and slang should not be used.

Users should not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, Users should not employ passwords like "X21JAN" in January or "X34FEB" in February.

Users should not use their Social Security numbers as passwords or any number derived from such, such as the last four digits of their Social Security number.

All User-chosen passwords must contain at least one:

- non-alpha character (*e.g.*, "1" or "#");

- upper case alpha character (*e.g.*, “A” or “Z”); and
- lower case alpha character (*e.g.*, “a” or “z”).

Users should not construct passwords that are identical or substantially similar to passwords that they have previously utilized.

User passwords should be changed every 90 days and not reused until after four passwords have been used. In short, a password can be used only once per account per year. Different system accounts should have different passwords. User IDs and/or passwords are not to be written down and kept within the general area of the computer. Users may not utilize internal passwords or substantially similar passwords on external systems (*i.e.*, websites, web-based email, etc.).

A User must promptly change his or her password if the password is suspected of being disclosed or known to have been disclosed to another individual.

Related Policies in this Handbook:
Information Security & Technology Resources
Electronic Access Controls

Encryption Policy

All passwords/encryption keys should be on file by the User with an authorized representative of ITS prior to their use.

Please contact the ITS Help Desk by calling #6123 from campus phones or (212) 960-5294 from non-campus phones or by email at helpdesk@yu.edu for more information on encryption options.

Related Policies in this Handbook:
Protection of Confidential Information and Personal Information

Anti-Virus Protection

All computers, including a User’s personal computer(s), that connect to the Technology Resources must have anti-virus and anti-spyware/malware software correctly installed, configured, activated and updated with the latest version of virus definitions prior to use. This software is to remain activated with the most up-to-date virus definitions files at all times. An authorized representative of ITS will ensure that the software is updated as appropriate on University-owned Technology Resources. This will be accomplished wherever possible by using the approved, centrally administered anti-virus software and by configuring these systems to automatically receive the most current updates from a central server. For non- University-owned Technology Resources, the ITS Help Desk can provide Users with anti-virus software.

A User should notify the ITS Help Desk by calling #6123 from campus phones or (212) 960-5294 from non-campus phones or by email at helpdesk@yu.edu if his or her anti-virus protection software is not working or if a device becomes infected with a virus. If a User suspects there is a virus, the User should immediately stop using the PC, note the symptoms and call ITS.

If a computer becomes infected with a virus or other form of malicious code, ITS will determine whether the computer must be disconnected from the University network until the infection has been removed in order to protect Yeshiva University Information and Technology Resources and assist the User in removing the virus. ITS will endeavor to promptly notify the User of such action.

Users may not intentionally write, generate, compile, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of any computer's memory file system or software.

Related Policies in this Handbook:
Electronic Access Controls

Reports of Lost Equipment or Potential Security Breaches

Users who suspect the loss or theft of any electronic equipment or any breach of the confidentiality or security of Confidential Information or Personal Information, must immediately contact the ITS Help Desk by calling #6123 from campus phones or (212) 960-5294 from non-campus phones. Users may also send an email directed to abuse@yu.edu to report the loss, theft or breach.

BlackBerry handhelds, smartphones and other PDAs may contain Confidential Information and Personal Information in the form of the University's internal contact list or in email messages and their attachments. Call the ITS Help Desk at #6123 or (212) 960-5294 immediately if a University-owned BlackBerry handheld, smartphone or other PDA is lost. The unit's data will be wirelessly erased to minimize the risk of disclosure.

Related Policies in this Handbook:
Information Security & Technology Resources
Physical Security of Technology Resources
Laptops and Portable Devices

Technology Resources Disposal

Information of a sensitive nature that is discarded inappropriately may fall into the wrong hands. All Users must ensure that any Technology Resources to be discarded that

contains Highly Sensitive or Confidential Information (in whole or part) will be properly destroyed and cannot simply be given away or deleted. Electronic media containing Highly Sensitive Confidential Information should be erased or destroyed to render them unreadable.

The destruction of electronic media presents data security concerns and environmental concerns. **Only ITS** is authorized to dispose of University-owned electronic media. Data on all University-owned electronic media such as disk drives, tapes, cd-roms, flash memory, etc., must be destroyed prior to disposition either by destruction of the media or destruction of the data which ensures the data cannot be recovered. An authorized representative of ITS will ensure that data on all electronic media to be discarded or sent out of house for repair will have all Highly Sensitive, Confidential Information or Personal Information thoroughly removed from it or securely and permanently disabled. All hardware must be disposed of through approved electronic equipment recyclers.

Note Regarding Deleted Information

Deleting information, Documents or messages does not mean that the information, Documents or message are really gone. Any information kept on the Technology Resources may be electronically recalled or reconstructed, regardless of whether it may have been "deleted" by a User. Because there are backups on tape of all files and messages, and because of the way in which computers reuse file storage space, files and messages may exist that are thought to have been deleted.

All Users should exercise care in what information or statements they create in electronic form to avoid potential embarrassment or legal liability for themselves or the University.

Related Policies in this Handbook:
Information Security & Technology Resources
Document Retention

Remote Access

Remote access connection to the University's network is allowed only through University-approved remote access technologies. All remotely connected devices must adhere to the University's anti-virus and security policies.

A User of a remote connection must:

- follow all University policies and procedures related to remote access;
- use a machine that has up-to-date anti-virus software running;
- not allow any File sharing or peer-to-peer program to be downloaded or running on the machine used to connect remotely, except where needed for University-support purposes; and

- report any observed or suspected violations of University policies and procedures related to remote access to the network.

Related Policies in this Handbook:
Information Security & Technology Resources
Anti-Virus Policy
Work Outside of Yeshiva University's Premises
Laptops and Portable Devices

Work Outside of Yeshiva University's Premises

When working outside of YU's premises, each User must:

- take steps at all times to protect YU's hardware, software and Information from theft, damage and misuse and unauthorized access or acquisition; and
- only keep, access and transport records containing Confidential Information or Personal Information when such Information is necessary in order for the employee to perform his or her job responsibilities outside of University premises.

Related Policies in this Handbook:
Information Security & Technology Resources
Physical Security of Technology Resources
Remote Access
Laptops and Portable Devices

Laptops and Portable Devices

Physical Security

When in the office, University-owned laptops and docking stations should be secured to an immovable object via the provided Universal Security Slot ("**USS**") locking mechanism. Please contact the ITS Help Desk if a locking mechanism is needed.

Users are responsible for their University-owned laptops and other portable devices outside the University's buildings. Never leave a laptop or other portable device unattended, even for a few minutes, particularly in public places, such as at airports or on a train. In addition, laptops should not be checked as or with luggage on airplanes.

Automatic screen locking mechanisms and boot passwords should be used where possible.

Technical Security

University-owned laptops and portable devices should be password-protected with device lockout set for a minimum of 15 minutes. Data encryption should also be used where technically possible for all laptops and portable devices.

Each User who has been provided a University laptop or other portable device must:

- avoid placing Highly Sensitive Information on any laptop or portable device, unless the device is encrypted;
- minimize the amount of Confidential Information and Personal Information on the laptop or portable device to the amount reasonably necessary to perform the User's job duties;
- not use any option that "remembers" passwords;
- switch off the laptop or portable device when not in use;
- not tamper with anti-virus software and other security tools installed on the laptop or portable device; and
- never store passwords for any Technology Resource on the laptop or portable device.

Related Policies in this Handbook:
Information Security & Technology Resources
Physical Security of Technology Resources
Anti-Virus
Remote Access
Work Outside of Yeshiva University's Premises

Electronic Mail (Email)

Email is an important business communication tool, and the number of email messages being transmitted and stored on email servers continues to increase. The cost of storing and managing emails continues to rise, and, thus, it is important that the drafting, transmitting and storing of emails are done with care.

All email, SMS or text communications sent over or stored on Yeshiva Universities Technology Resources are the exclusive property of Yeshiva University. Yeshiva University may review email, SMS, text or similar communications at any time, for any purpose.

Composing Emails

Emails are just like any other document prepared in the course of Users' work for Yeshiva University. Emails should reflect the care and precision of all written communications relating to the business activities of Yeshiva University.

Users should spell check all emails prior to sending. Emails should not be written entirely in capital letters.

Strictly avoid any statements that could be viewed as defamatory or slanderous of Yeshiva University's services, employees, other organizations' products or services, students or other third parties, or otherwise unlawful or contrary to Yeshiva University's policies or business interests. If a User receives an email of this nature, he or she must promptly notify his or her supervisor.

Given their nature, emails are sometimes distributed inadvertently. Emails may end up being seen or used in unforeseen ways. It is imperative that a User ensures that the contents of emails are accurate and appropriate, based on the facts. Please avoid exaggerations and expressions that may be misinterpreted. Emails are not private. For example, emails sent within or outside of Yeshiva University are discoverable in litigation and may be used as evidence against Yeshiva University. If a message needs to be confidential, carefully consider if an email is the most appropriate form of communication.

Users should only mark emails as important if they really are important.

Sending Emails

When sending emails, select the recipients cautiously and do not add recipients to the "to," "cc," or "bcc" lines without careful consideration. Check the recipient's email address to ensure that it does not contain any error.

When sending a reply email or forwarding an email, avoid including the list of email addresses from the original email.

Forwarding emails requires special caution. Users should clearly state what action they expect the recipient to take on forwarded emails. Before forwarding an email, or replying with a copy to a new recipient, check the email series and any attachments to make sure that it is appropriate to share the content with the new recipient. Consider whether any attachments from the original email are necessary, and remove them if they are not important or necessary. Compress attachments larger than 1 MB before sending them.

In addition, Users may not:

- Forge or attempt to forge email messages;
- Disguise or attempt to disguise his or her identity when sending emails;

- Send or receive email messages using another person's email account;
- Subscribe to any email lists that are not directly relevant to his or her assigned duties;
- Create or forward solicitations, including those for charitable contributions or product sales, or "chain letters;"
- Intercept, copy, alter or interfere with the sending or receiving of email within Yeshiva University's Technology Resources without the written approval of an authorized representative of ITS;
- Copy a message or attachment belonging to another User and forward it as his or her own work product without permission of the originator;
- Attempt to access another User's email or files or any other information in the Technology Resources to which he or she does not have authorized access;
- Provide mailbox access to others, except where such access is approved by an officer of Yeshiva University;
- Forward or send copyrighted materials unless he or she has the author's permission; or
- Send any message which may be deemed to constitute unlawful harassment (including sexual harassment).

In addition, due to the potential for security breaches, Users must exercise extreme caution in downloading and executing any files attached to email. Attachments that are not clearly business-related and/or expected from a known source should never be opened or executed. Such emails and attachments should be immediately forwarded to an authorized representative of ITS.

Signatures

All YU business-related emails, including emails sent from a BlackBerry or other PDA, that are addressed to any person(s) outside of Yeshiva University must clearly identify the User by full name and official title. The User's telephone number and the Users' department signature with all appropriate disclaimers must also be included.

All incidental non-business email must contain the following statement: "This is a personal email. Any opinions, statements, advice, or recommendations contained in this email are my own and do not reflect those of Yeshiva University."

Managing and Saving Emails

Email is permanent. Although a User may send emails and may delete emails from his or her Sent box, emails may not really be deleted. A copy of each email a User sends is saved in the University's servers. And even if a User deletes the email, a copy still resides in the servers. Thus, Users must consider the content of each email before they push the send button.

Please ensure that emails are retained and disposed of in accordance with any policies promulgated by the University's Office of the General Counsel (*e.g.,* Yeshiva University Record Retention Policy).

If litigation is likely to be filed or has been actually filed, emails relating to such litigation or potential litigation must be saved until the litigation proceedings are over. Please save relevant emails in accordance with the instructions of the University's Office of the General Counsel or the respective manager.

Related Policies in this Handbook:
Installation and Use of Software
Privacy
Protection of Confidential Information and Personal Information
Internet Access and Use

See also Yeshiva University Record Retention Policy and Yeshiva University Harassment Policy and Complaint Procedures

Internet Access and Use

Each User is responsible for ensuring that his or her use of YU's Internet access is consistent with this Handbook, any other applicable University policy, and appropriate business practices. All access to the Internet should use University-supported browsers.

The University may review Internet use, including the amount of time spent on the Internet and sites visited, at any time, for any purpose.

Users should be mindful that Internet sites they visit collect information about visitors. This information will link the User to YU. Users may not visit any site that might in any way cause damage to YU's image or reputation.

Internet sites containing pornography, sexist material, racist material, obscene material, pirated software, or any other inappropriate material shall not be accessed unless with the specific permission of the Vice President of ITS, or his or her designee. Further, Internet access shall not be used for any purpose in violation of law, rule or regulations.

In addition, Users may not (unless related to an authorized University business purpose):

- Change any YU browser security settings;
- Use Technology Resources to deliberately propagate any virus, worm, Trojan horse, trap-door program code or any unauthorized Internet service;
- Post any comments or statements on any web page or send any messages to Internet newsgroups without prior written authorization from an authorized representative of ITS; or

- Download files from the Internet, including web browser add-ins or other such software providing search bars, weather, and screensavers, unless prior written approval has been obtained from an authorized representative of ITS.

Users should be aware that much of the material available on the Internet is copyrighted or trademarked. Other than viewing publicly available material, Users may not use any material found on the Internet in any manner without first establishing that such use would not be in violation of a copyright, trademark or other intellectual property and proprietary rights.

Related Policies in this Handbook:
Using Technology Resources
Installation and Use of Software
Privacy
Use of Copyrighted Material
Electronic Mail (Email)
Social Media Policy

See also Yeshiva University Harassment Policy and Complaint Procedures

Social Media Policy

Social media can be a valuable and powerful means of communication. The University would like Users to keep the following guidelines in mind when participating in social media to protect Users' interests, as well as YU's interests. For purposes of these guidelines, all such activity is referred to as "posting," and "social media" includes social and professional networking sites and other participatory online media hosted by third parties where written information and other content, like photographs, videos, and audio files, are posted and published by users (who may include site administrators as well as independent third party end users) using tools such as profiles, message boards, wikis, blogs, picture sharing networks, and online communities. Examples of social media include, but are not limited to, Facebook, Ning, Twitter, YouTube, and Flickr.

General Guidelines for Participating in Social Media

Be careful about the content of posts. Each User is personally responsible for what he or she posts. Remember that anything a User posts may be public for a long time, even if the User tries to modify or remove it later. YU disclaims any responsibility or liability for any errors, omissions, loss, or damages claimed or incurred due to any postings of a User.

Speak for yourself, not the University. This includes the following:

- Other than when Users are speaking on behalf of the University with appropriate authorization, Users who identify themselves as YU staff or

comment on a University-related issue while posting must include a prominent disclaimer stating that the views being expressed are the User's own, and not necessarily YU's views.

- Users may not use YU's logo or other marks, and must make certain that their choice of words does nothing to suggest that they are representing the University's official position, in each case, unless the Users have been authorized by YU's Office of Communication and Public Affairs to do so; questions regarding the use of University logos and other marks should be directed to the University's Office of the General Counsel.
- If a member of the media contacts a User to comment upon YU or any University affairs, please refer that person to YU's Office of Communication and Public Affairs.
- In general, personal social media activity should be kept distinct from professional social media activity, and communications with purely personal social media sites should be conducted from personal email accounts only.

Protect Confidential Information and Personal Information. Users should not post Confidential Information or Personal Information, and ensure that their online contributions comply with Health Insurance Portability and Accountability Act (HIPAA) and Federal Education Records Protection Act (FERPA) requirements. Users should not post at all while attending business meetings.

Respect University policies. Users' postings should not violate any other applicable University policy.

Limit time online while at work. Social media use that qualifies as Incidental Personal Use is allowed; however, Users may not remain logged in to social media accounts all day. In addition, Users may not allow their use of social media sites to interfere with their job responsibilities.

Be respectful of others. Users should be professional and respectful of others in their communications, and refrain from posting statements that are false, misleading, obscene, defamatory (whether of YU or its employees, students or competitors), libelous, tortious, degrading, threatening, harassing, hateful, insulting, inflammatory, offensive, unlawful, fraudulent, discriminatory, or invasive of the privacy of others.

Respect laws. Respect copyright, trademark, privacy, financial disclosure, and all other laws. Users may not disclose Personal Information about other individuals that may have been obtained through their work at YU. In accessing or using a social media site, do not engage in violations of the legal terms, codes of conduct, or other requirements, procedures, or policies of or governing such site. Do not post materials of others – such as photographs, articles, or music – without first getting their permission. Users should attribute what they post; let others know where they get their information, being particularly respectful of and compliant with copyright, trademark, and other intellectual property and proprietary rights. Be careful about "reposting"

information from other sites. Also, do not comment on YU's confidential financial information, such as future business performance, business plans, or prospects, to anyone in any forum.

Report inappropriate conduct. If a User feels that agents of the University are, have been, or will be engaged in any inappropriate conduct, the User should discuss his or her concerns with a representative of YU's Human Resources department rather than publicizing suspicions or making allegations through posting.

Passwords. It is the User's responsibility to maintain the security of the password he or she uses to access a social media site (or features contained on such site).

Privacy. In accessing or using a social media site, Users should review such site's Privacy Policy to understand how the site uses the information that Users provide. Be careful about revealing excessive personal information, including birth date, contact information, and personal pictures. Users who do not want their information to be publicly available should not post it online. Because YU retains the right (but not the obligation) to monitor all files and messages stored on and transmitted through YU's computers, remember that Users have no reasonable expectation of privacy on social media accessed through the Technology Resources, even if Users have used a private account.

Endorsements. If someone offers to pay a User for participating in social media in or in connection with his or her role as a member of University staff, or offers to pay the User for or in connection with advertising or endorsements, this could create a conflict of interest. Please contact the University's Office of the General Counsel for further information.

Special note for managers. Managers must take special care when posting and be thoughtful about how they present themselves as members of the YU staff. Due to the nature of their positions, their personal postings may be interpreted as the views and opinions of, and will reflect on, the University even with standard disclaimer language in place.

Keep current. These guidelines may evolve as new technologies and social media tools emerge. Users must check this policy periodically to ensure that they are familiar with its content.

Establishing a University-Related Social Media Profile. If a User wishes to establish a University-related presence on a particular social media site or service, please refer to the University's *Guidelines Concerning University-Related Social Media Profiles* for additional information.

Related Policies in this Handbook:
Internet Access and Use
Password Policy

See also Guidelines Concerning University-Related Social Media Profiles

Document Retention

All Documents will be maintained for the duration established by the University's Office of the General Counsel. Immediately upon expiration of the appropriate document retention period, all copies of the Document (physical and electronic) will be destroyed. Information must be destroyed in a manner consistent with the information's level of sensitivity. For example, Users should not place Technology Resources containing Confidential Information or Personal Information in garbage or recycling bins. Instead Users should contact ITS in compliance with the Technology Resources Disposal policy set forth in this Handbook.

If a User is notified by the University that the University is involved in or subject to an imminent official investigation, litigation, or legal document request, *all Document destruction must cease immediately*. Do not resume Document destruction until specifically instructed by the University's Office of the General Counsel or ITS. Failure to comply with document retention protocols may result in fines, penalties, or sanctions against the User and/or the University.

Related Policies in this Handbook:
Protection of Confidential Information and Personal Information
Technology Resources Disposal

Compliance and Penalties

All Users must comply with all applicable policies that YU has implemented and may implement from time to time, including this Handbook and all other University policies. Failure to comply with this Handbook or other University policy may result in disciplinary action as more fully described in the University's Employee Handbook and/or other Human Resources policies.

USER ACKNOWLEDGMENT

PLEASE READ THE YESHIVA UNIVERSITY STAFF TECHNOLOGY RESOURCES USE HANDBOOK, AND FILL OUT AND RETURN THIS PORTION TO THE HUMAN RESOURCES DEPARTMENT WITHIN ONE WEEK OF EMPLOYMENT.

I acknowledge that I have received a copy of the Yeshiva University Staff Technology Resources Use Handbook. I understand that I am responsible for reading the Handbook and for knowing and complying with the policies set forth in the Handbook during my employment with Yeshiva University.

I understand that the University has the right to amend, interpret, modify, or withdraw any of the provisions of the Handbook at any time in its sole discretion, with or without notice. Furthermore, I understand that because the University cannot anticipate every issue that may arise during my use of the Technology Resources (as defined in the Handbook), if I have any questions regarding any of the University's policies or procedures, I should consult the University's Information Technology Services Department.

_____
Signature

_____
Printed Name

_____
Title

_____
Date

RECOMMENDED PRACTICES FOR EMAIL COMMUNICATIONS

- **Think before sending an email.** While the University encourages the use of email for short informal communications, it is important to remember that emails are business documents that deserve the same degree of care as formal memoranda or letters. A momentary lapse of judgment before clicking the “send” button can have long-term and unintended consequences.
- **Maintain professionalism.** Email should not be used to forward jokes, post items on chat rooms, or gossip. Emails should be well-structured and include short, descriptive subject-lines. Although we tend to be more casual in emails, Users should not write in emails things that would not be appropriate in a formal memo. Sarcasm, slang, inside jokes, smiley faces and the like might be understood by the recipient, but they can take on unintended meanings when viewed by an outsider. The tone of a User’s emails should be consistent with the User’s level of responsibility at the University.
- **Respond promptly**. Emails should be answered as soon as reasonably practicable and generally within 2 working days.
- **Check the recipients before sending email.** Many embarrassing moments are caused by accidentally clicking "reply all" when intending to respond only to the prior sender, or clicking "reply" instead of "forward" when intending to communicate with someone other than the sender. It is always a good idea to check the recipients listed on a message before clicking "send." When replying to a received email, consider whether anyone other than the person who sent the email should receive a copy of the reply. Users should avoid using “reply all” unless they have concluded that all of the recipients should receive a copy of the reply.
- **Delete emails.** Appropriately review emails saved on servers, personal computers, recording media or elsewhere to determine whether they are necessary for the business of YU, and promptly delete any emails that are no longer necessary (subject to the University’s Record Retention Policy).