Yeshiva University Student Technology Resources Use Handbook

INTRODUCTION **1**

Definitions 1

Using Technology Resources 2

Privacy 2

Installation and Use of Software 3

Use of Copyrighted Material 3

P2P File-Sharing Policy 4

Information Security & Technology Resources 5

Physical Security of Technology Resources 6

Electronic Access Controls 6

Password Policy 7

Anti-Virus Protection 8

Reports of Potential Security Breaches 8

Note Regarding Deleted Information 8

Remote Access 9

Electronic Mail (Email) 9

Internet Access and Use 11

Social Media Policy 11

Compliance and Penalties 12

USER ACKNOWLEDGMENT **13**

INTRODUCTION

Yeshiva University ("YU" or the "University") provides various technology resources, including computers, Internet access, email, and telephones to its staff, faculty and student body ("Users") to facilitate the exchange of ideas and information, and to aid in the University's communications and work-related research. Use of these resources is governed by the University's policies, including this Handbook, and applicable laws.

It is important for all students to read and understand these policies. Policy violations may have serious consequences for a User's access to resources and also his or her University career.

The University reserves the right to revise and modify the policies contained in this Handbook. Questions concerning the policies and procedures and their applicability should be addressed to the University's Information Security Administrator at infosec@.yu.edu. Any clear misuse of University computers or computing resources or evidence of intrusions or tampering should be reported by email to abuse@einstein.yu.edu or abuse@yu.edu.

Definitions

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.

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 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 Yeshiva University's 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 Yeshiva 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 Yeshiva University's network and access to outside sources of information such as the Internet.

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

User(s): all Yeshiva University students with access to Technology Resources.

Using Technology Resources

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

Users may not use the Technology Resources for commercial purposes. In addition, Users may not use the Technology Resources to commit any illegal act; or harass an individual or organization.

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 University's Technology Resources. The University 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 its Technology Resources.

Privacy

The University may inspect all files or messages on its Technology Resources at any time for any reason at its discretion. The University may also monitor its Technology Resources at any time to determine compliance with its policies, answer a lawful subpoena or court order, investigate misconduct, locate information, or for any other operational purpose.

The University makes every effort to ensure that information and messages stored and transported on its Technology Resources are safe from unauthorized use or examination. However, Users should not assume that information or messages stored or transported on the

University's Technology Resources are safe from unauthorized access. Users can contribute to ensuring the privacy of student and University information by following these policies and the Security Policies.

Related Policies:
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 approved and controlled by ITS. It is the University's policy that all software in use on its Technology Resources is officially licensed. An authorized representative of ITS will ensure that all software installed or utilized on Yeshiva University machines 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, you may not:

- install any software on University-owned computer equipment;
- 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:
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. 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 law and this Handbook, you 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 network except as authorized by ITS in writing.

An authorized representative of ITS shall ensure that all copyrighted material found or used on University machines is properly licensed. For more information on the University's policies

regarding copyrights, please see the University Digital Millennium Copyright Act (DMCA) policy available in the ITS Information Security office.

Related Policies:
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, accidental or intentional, no P2P software may be used on or in connection with Yeshiva University's Technology Resources, and such 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's 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's 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 networks may result in disciplinary action or termination of access.

Related Policies:
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 University information, regardless of its form (e.g., paper and electronic records). Users are responsible for preventing unauthorized access to, and protecting the security and confidentiality of University information stored on Technology Resources.

Please see **[GENERAL UNIVERSITY POLICY ON INFORMATION SECURITY]**

You are required to protect your individual passwords from unauthorized use or access. You may not disclose your login IDs or 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.

Related Policies:
Physical Security of Technology Resources
Electronic Access Controls
Password Policy

Physical Security of Technology Resources

University-owned computer equipment may not be removed from the University's premises without the prior written authorization of an authorized representative of ITS. Users may not modify the University's Technology Resources 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, such as a wireless router. ITS will authorize all User modifications that may be necessary for academic purposes.

If a User connects his or her personal computer equipment to the University's Technology Resources, the User is responsible for the security of that equipment. Any misuse of the University's Technology Resources due to a User's neglect may result in the University denying that User access to the Technology Resources.

Related Policies:
Information Security & Technology Resources
Electronic Access Controls
Password Policy

Electronic Access Controls

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

- test or attempt to compromise internal and preventive controls of any University Technology Resources, 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 that Users have been authorized to obtain;
    - taking resources away from other Users; or
    - gaining access to Technology Resources for which proper authorization has not been granted.

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

Students should also take other precautions to protect their own personal computers:

- Use password-protected screensavers.
- Do not install any P2P software.
- Ensure that the computer is not configured to allow other devices unauthorized access to YU's networks.

Password Policy

Where technically possible, all passwords allowing access to Technology Resources must be at least eight (8) characters in length. Users must choose passwords that cannot be easily guessed. Passwords should not be related to a User's job or personal life. For example, a car license plate number, a girlfriend or boyfriend's name or an address should not be used. Passwords also should not be words found in the dictionary. For example, 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.

A User's 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").

A User should not construct passwords that are identical or substantially similar to passwords that you have previously used.

A User's passwords must be changed every 90 days and may not be reused until after 4 passwords have been used. In short, a password can be used only once per account per year. Different system accounts should have different passwords. A User should not use Technology Resources 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:
Information Security & Technology Resources
Electronic Access Controls

Anti-Virus Protection

All computers, including a User's personal computers, 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 definition files at all times. The ITS Help Desk can provide you 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 a device becomes infected with a virus. 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 network until the infection has been removed in order to protect University information and Technology Resources and assist the User in removing the virus.

A User 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.

A User should use the Internet in a responsible manner and should avoid browsing or accessing inappropriate sites that might expose his or her computer and, consequently, the University's Technology Resources, to viruses and similar threats.

Related Policies:
Information Security & Technology Resources

Reports of Potential Security Breaches

Users who suspect a breach of the confidentiality or security of Personal Information in relation to Technology Resources must immediately inform 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 incident.

Related Policies:
Information Security & Technology Resources

Note Regarding Deleted Information

Deleting information, documents or messages does not necessarily mean that the information, documents or messages are really gone. All members of the University community should understand that 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.

Remote Access

Remote access connection to the University 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 P2P 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 the University's policies and procedures related to remote access to the network.

Related Policies:
Anti-Virus Policy

Electronic Mail (Email)

Email is an important communication tool and one of the primary means of communication among members of the University community. This policy sets forth the practices and expectations for the use of email on the University's Technology Resources.

Email Access

ITS assigns a login ID to every student registered in a degree program at the University. This login ID will become part of the User's University email address.

Students at the University are expected to actively maintain a University email account at which they will receive University communications. Students are expected to check their email accounts on a regular basis to stay current with communications from the University.

Email Use

When using the University's email system, Users are prohibited from:

- Forging or attempting to forge email messages;

- Disguising or attempting to disguise your identity when sending email;
- Sending or receiving email messages using another person's email account;
- Creating or forwarding solicitations, including those for financial gain, or "chain letters";
- Intercepting, copying, altering or interfering with the sending or receiving of email within the University's Technology Resources;
- Copying a message or attachment belonging to another User and forwarding it as work product without permission of the originator;
- Attempting to access another User's email or files or any other information in the Technology Resources without authorized access;
- Providing mailbox access to others, except where such access is approved by an officer of University; or
- Forwarding or sending copyrighted materials without the author's permission.

Email Guidelines

Emails are just like any other document prepared by a User in the course of that User's University career. Email may be used as an official means of communication between a User and the faculty or a User and the University. Although people tend to be more casual in emails, consider following these guidelines in email communications:

- Spell check emails prior to sending;
- Avoid writing emails entirely in capital letters;
- Only mark emails as important if they really are important;
- Emails may be vulnerable during transmission and after they have been received by the recipient. Avoid sending sensitive information in an email;
- Check the recipient's email address to ensure that it does not contain any error;
- Make sure that before using "reply all," you intend to send the message to *all* listed recipients; and
- Exercise extreme caution in downloading and executing any files attached to email. Attachments that are not 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.

Internet Access and Use

Users are responsible for ensuring that use of the University's Internet access is consistent with this Handbook, any other applicable University policy, and appropriate business practices.

Internet access shall not be used for any purpose in violation of laws or regulations. In addition, Users may not:

- Change any University browser security settings on University-owned Technology Resources;

- Use Technology Resources to deliberately propagate any virus, worm, Trojan horse, trap-door program code or any unauthorized Internet service.

Related Policies:
Using Technology Resources
Privacy

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 the University'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

Be careful about what you post. 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. The University disclaims any responsibility or liability for any errors, omissions, losses, or damages claimed or incurred due to any of a User's postings.

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

- If the User identifies himself or herself as associated with the University or comments on a University-related issue while posting, the User should identify him or herself as a student.
- A User may not use the University's logo, and must make certain that his or her choice of words does nothing to suggest that he or she is representing the University's official

position, unless the User has been authorized to do so by the Department of Communications and Public Affairs.

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

Be respectful of others. Users should be respectful of others in all communications, and refrain from posting statements that are false, misleading, obscene, defamatory, 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. In accessing or using a social media site, Users should 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. Attribute what you post; let others know where you get your 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.

Passwords. Users are responsible for maintaining the security of passwords used 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 your birth date, contact information, and personal pictures. Users who do not want their information to be publicly available should not post it online.

Related Policies:
Internet Access and Use
Password Policy

Compliance and Penalties

All students must comply with all applicable policies that the University has implemented and may implement from time to time, including this Technology Resources Use Handbook and the rest of the University's policies.

Damage to or loss of Technology Resources caused by negligence and/or violation of this Handbook may result in the responsible party being charged for the repair or replacement costs. Further, if a User fails to comply with this Handbook, or any other University policy, the User will be subject to disciplinary action by the appropriate disciplinary authority up to, and including, loss of Technology Resources access rights, suspension or expulsion.

USER ACKNOWLEDGMENT

PLEASE READ THE STUDENT TECHNOLOGY RESOURCES USE HANDBOOK AND FILL OUT AND RETURN THIS PORTION TO ITS.

I acknowledge that I have received a copy of Yeshiva University's 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 studies at Yeshiva University.

I understand that Yeshiva 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 Yeshiva University cannot anticipate every issue that may arise during my use of the Technology Resources, if I have any questions regarding any of Yeshiva University's policies or procedures, I should consult Yeshiva University's Information Technology Services Department.

_____
Signature

_____
Printed Name

_____
Title

_____
Date