Information Technology Services

YU Student IT Handbook

Contacting Support:

ITS Help Desk, helpdesk@yu.edu, 800-337-2975 or 646-592-4357, Teams dial 4357

[Updated February 15th, 2022]

Table of Contents

Purpose

Yeshiva University ("**YU**" or the "**University**") provides various technology resources, including computers, Internet access, and email to the University's students to facilitate the exchange of ideas and information, and to aid in the University's communications and academic work. Use of these resources is governed by the University's policies, including this Handbook, and applicable laws.

It is important for all Users (defined below) to read and understand this Handbook and the policies contained herein. Policy violations may have serious consequences for a User's access to resources and their University career. Student employees must also read and understand the YU Administration, Faculty and Staff Handbook, and comply with the policies contained therein when acting in their capacity as a student employee.

The University reserves the right to revise and modify the policies contained in this Handbook in its sole discretion. 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.

Definitions

Term	Definition
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 University's Information Technology Services Department
Peer-to-Peer (P2P)	Software, services, and protocols that are commonly referred to as "peer-to-peer" or "P2P," such as BitTorrent. 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.
Technology Resources	Consists of all University-owned personal computers and workstations, including notebook and laptop computers; peripheral equipment such as monitors, keyboards, mouse, printers, telephone equipment; smartphones; computer software applications and associated files and data; direct (wired and wireless) and remote access to the University's network; and access to outside sources of information such as the Internet.
University Community	All University administration, staff, faculty and students
User(s)	All University students with access to Technology Resources.
Yeshiva University Information	Any information that is collected, used or maintained by the University. Yeshiva University Information may include all Confidential Information or Personal Information (including Highly Sensitive Information).

Policy

Introduction

It is important for all Users to read and understand this Handbook and the policies contained herein. Policy violations may have serious disciplinary consequences, including loss of access to Technology Resources.

All information stored, transmitted, or handled by the Technology Resources is the property of the University. Subject to applicable law, authorized University personnel may review and monitor this information at any time without the User's permission.

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. 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.

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, however, all communication used by a YU-owned email account is owned by YU. Users have no expectation of privacy using YU email or Technology Resources.
- use computers and smartphones 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).
- participate in University-sponsored Internet communities within defined guidelines.

Users are prohibited from using Technology Resources for:

- 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 prohibited.

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 authorized University personnel at any time without User 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 transmitted on the Technology Resources are safe from unauthorized use or examination. Users should not, however, assume that information or messages stored or transmitted on the Technology Resources are safe from unauthorized access.

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 YU's policy that all software in use on the Technology Resources is officially licensed to YU. The User 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.

All Users are expected to cooperate with ITS to ensure that all copyrighted material found or utilized on the Technology Resources 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, as well as disciplinary action.

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). P2P software, when abused, can saturate an entire network and leave some or all of its users with poor to non-existent performance. Additionally, P2P software is frequently used for the transfer of copyrighted materials (such as music and movies) in violation of the Yeshiva University Digital Millennium Copyright Act (DMCA) policy.

In order to prevent any type of abuse or infringement (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 coursework 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 ticket to 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 their 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 has 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 to Technology Resources.

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

Information Security & Technology Resources

All Users 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 should not disclose their YU credentials to anyone. There are no exceptions. If a legal, harassment, or other complaint or charge is made against a specific YU credential, the owner of those credentials is liable.

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 they need the User's login ID and password. **Members of ITS will never call a User and ask for a login ID and password. NEVER!**

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.

Related Policies in this Handbook:

Password Policy

Physical Security of Technology Resources

Users must ensure that they use all Technology Resources (desktop computers, monitors, laptop computers, printers, phones, etc.) 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. Only modifications determined by ITS to be necessary for business or academic purposes will be authorized.

If a User connects their personal computer equipment to the Technology Resources, the User is responsible for the security of that equipment. Any misuse by a User of the Technology Resources, whether intentional, negligent, or otherwise, may result in the University denying that User access to the Technology Resources.

See also: Bring Your Own Device (BYOD) 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 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 they 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.

Any misuse of University computers or computing resources, or evidence of intrusions or tampering, should be promptly reported by email to abuse@yu.edu.

All University-owned computers should have personal firewall software installed. Users may not modify this software; it 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 owned or otherwise controlled by the University , 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 owned or otherwise controlled by the University 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.

Users 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.

Related Policies in this Handbook:

Password Policy
Anti-Virus Protection
See also: Network Accessible Use policy and Bring Your Own Device (BYOD) Policy

Password Policy

Users must comply with all applicable guidelines promulgated from time to time by ITS in selecting passwords (including, without limitation, the length of the password). 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 them, such as the last four digits of their Social Security number.

All User-chosen passwords must contain several:

- non-alpha characters (*e.g.*, "1" or "#");
- upper case alpha characters (*e.g.*, "A" or "Z");
- and lower case alpha characters (e.g., "a" or "z").

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

Different system accounts should have different passwords. User IDs and/or passwords should not be written down and not 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 their 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

Anti-Virus Protection

All User's 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 (without User modification) with the most up-to-date virus definitions files at all times.

A User should notify the ITS Help Desk if the antivirus protection software is not working or if a device becomes infected with a virus. If a User suspects there is a virus on Technology Resources, the User should immediately stop using the computer, note the symptoms and call the ITS Help Desk.

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.

A User should use the Internet in a responsible manner and should avoid browsing or accessing inappropriate sites, and further should avoid opening attachment/files or clicking links in unknown/unexpected emails, that might expose their computer and, consequently, the Technology Resources, to viruses and similar threats.

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 Yeshiva University Information should immediately contact the ITS Help Desk. Users may also send an email directed to abuse@yu.edu to report the loss, theft or breach.

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

Remote Access

At this time, Users have no access to the Remote access connection (VPN) to the University's network.

Laptops and Portable Devices

Physical Security Guidelines

Users should 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.

Bring Your Own Device (BYOD) Policy

Many Users bring their own personal computing devices for use and studying at YU. Please see the Bring Your Own Device (BYOD) Policy for rules governing your use of Technology Resources while using your personal computing devices.

Electronic Mail (Email)

The University's Learning Management System (LMS – currently Canvas), and not email, should be used for student submissions.
ITS assigns email to every student registered in a degree program at the University. Students 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 their identity when sending email;
- Sending or receiving email messages using another person's email account;
- Intercepting, copying, altering or interfering with the sending or receiving of email within the 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;
- Forwarding or sending copyrighted materials without the author's permission; or
- Sending any message that may be deemed to constitute unlawful harassment (including sexual harassment).

Personal Use

Personal use of a University email account is permitted as long as it does not interfere with the University's needs or operations and is otherwise in compliance with University policies.

Ownership and Privacy

The University owns all University email accounts. Users do not have a personal privacy right in their University email accounts. Emails may be reviewed and monitored by University personnel at any time and for any reason without user permission.

Security

Incoming emails are scanned for viruses, phishing attacks and spam, and suspected emails are blocked. However, it is impossible to guarantee protection, and each User must use proper care and consideration to prevent the spread of viruses etc. Attachments that are not expected from a known source should never be opened or executed.

Specifically note emails that arrive and are tagged as coming from external users. Do not open attachments or follow links unless you are absolutely sure it is legitimate.

Passwords

Each user is responsible for his/her email account, including safeguarding of access, and should not share his/her password.

Questions

Questions or comments about this Policy should be directed to the Information Security division of the University's Information Technology Services (ITS) department at infosec@yu.edu.

Internet Access and Use

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

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 should not be accessed. Further, Internet access shall not be used for any purpose in violation of law, rule or regulations.

In addition, Users may not:

- Change any Technology Resource's settings;
- Use Technology Resources to deliberately propagate any virus, worm, Trojan horse, trap-door program code or any unauthorized Internet service;

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
Use of Copyrighted Material
Electronic Mail (Email)

Also: Yeshiva University Harassment Policy and Complaint Procedures

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, including termination of access to Technology Resources.

Penalties for Violation of Federal Copyright Law

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under Section 106 of the Copyright

Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment and fines.

For more information, please see the website of the U.S. Copyright Office at http://www.copyright.gov, and particularly, its FAQs at http://www.copyright.gov/help/faq.