Information Technology Resource Acceptable Use Policy

Effective Date	Responsible Officer	Responsible Office	This Policy Applies to:
07/01/2020	Vice President of Technology & Chief Information Officer	Division of Technology Services	All University departments and all faculty, staff, students, contractors, student employees, and anyone with access to University information technology resources.

I. POLICY STATEMENT

Wentworth University of Technology ("Wentworth") makes available information technology resources ("ITRs") to authorized faculty, staff, students, and other University community members for teaching, learning, research, administration and approved purposes. ITRs must be 1.) used in a manner that is consistent with University policies, standards, and applicable law and 2.) respectful of the rights of the Institution and the members of its community.

Wentworth only grants use, which shall be limited and conditional, of ITRs to appropriately authorized individuals who agree to the terms and conditions of this Acceptable Use Policy (AUP).

II. PURPOSE

Protecting the confidentiality, integrity, and availability of ITRs is a cooperative effort that requires each member of the Wentworth community to stay informed about University standards of acceptable and unacceptable ITR usage and communicate their concerns about unacceptable ITR usage to Wentworth.

III. SCOPE

This policy applies to all users of Wentworth ITRs, whether they are affiliated with Wentworth or not, and to all uses of those resources, whether on campus or from remote locations. This policy is supplemented by all other Wentworth policies, standards, and guidelines, and by the policies and standards of organizations with which Wentworth is formally affiliated, including – but not limited – to Colleges of the Fenway and related consortia.

Third-party service providers and contractors must communicate this policy to any of their workforce members who are authorized to access ITRs and monitor for compliance.

IV. DEFINITIONS

Information technology resources ("ITRs") are Wentworth owned, leased, and/or managed information, technology, or IT services, which include but is not limited to computer accounts (email, network, system, application, et al), computers (desktops, laptops, workstations, servers, classroom A/V, and all mobile devices), printers and other peripherals, telephones and facsimile machines, electronic technology (i.e., computer programs, folders, and files), local and wide area networks, Internet access, digital storage media, and any information that resides on or traverses these resources.

V. USER PRIVACY CONSIDERATIONS

The Wentworth information technology resources are the property of the University. Use of these resources is intended primarily for educational, scholarly and university business purposes. While technical staff and administrators will not casually or routinely monitor content or search files without a justified business cause, the University reserves the right to scan all network, systems, devices, as well as review any information stored or transmitted on this network, in response to a judicial order or other actions required by law or permitted by university policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the organization, without notice. Wentworth respects individual privacy, however, these information technology resources should not be considered private, and appropriate discretion should be used when sending and storing highly sensitive or confidential information.

VI. LOSS OF PERSONAL DATA

The University does not back up personal data (i.e., data created by an end user that is not for a sanctioned Wentworth business or academic purpose) from end user devices, such as laptop and desktop computers. Therefore, the University is not responsible for the recovery of personal data and will not satisfy requests to restore personal data. End users are advised to make backup copies of personal data on storage media they own and *not* on University provided ITRs.

VII. INCIDENT REPORTING

It is the responsibility of each member of the Wentworth community to report incidents involving violations of this and any University policy, as well as any unlawful activity, to the appropriate persons. For reporting incidents related to Wentworth information resources, email the Information Security Officer at infosec@wit.edu or call the Tech Spot at 617-989-4500. To report unlawful activity, contact Public Safety at 617-989-4400 or send an email to publicsafety@wit.edu.

VIII. EXCLUSIONS

This policy does not cover personally-owned information resources that are not connected to – nor otherwise make use of – ITRs. This policy also does not apply to cyber security, computer engineering, or network engineering research activity that, by its very nature, may violate the scope of this policy. All staff, faculty, or students involved in such research are strongly advised to consult with Wentworth's Information Security Officer before initiating any activities associated with such research to ensure that adequate and appropriate safeguards are implemented.

IX. RELATED DOCUMENTS

Document Name	Publisher[1]
Academic Catalogue *(current academic year)*	WIT
Policy on Accessing University IT Resources from Personally-owned Computing Devices	WIT
Stewardship of Information Policy	WIT
Student Code of Conduct	WIT

X. ENFORCEMENT OF POLICY VIOLATIONS

[1] For documents originating within WIT, such as policies or procedures, specify "WIT" and note if non-public. For other relevant third-party documents, such as external standards to which WIT subscribes, list the name of the organization that publishes the document.

Failure to comply with this policy, intentionally or unintentionally, may result in one or more of the following:

- Termination, without notice, of access privileges to information and technology resources.
- Disciplinary action, up to and/or termination of employment.
- Civil or criminal penalties as provided by law.

XI. REVIEW AND REVISION HISTORY

Policies must be reviewed annually by the policy owner. If a policy has been revised, then it must have all necessary approvals before being published. In the last column, indicate whether the activity was a review or a revision; if a revision, summarize the changes.

Date	Name and Title	Annual Review or Revision Summary
7/1/20	Bryce Cunningham, Information Security Officer	New policy issued by the IT and Security Policy Working Group (supersedes *Acceptable Use Policy*)
9/13/21	Bryce Cunningham, Information Security Officer	Added prohibition on employees auto forwarding emails to non-WIT email addresses and new Loss of Personal Data section stating that DTS does not backup personal computers.

APPENDIX: Standards of Acceptable Use of ITRs

A. Prohibitions: All ITR users must **not**:

1. Use or access computer or network services in a way that violates copyrights, patent protections or license agreements, such as using Peer-to-peer sharing of copyrighted- protected material.
2. Attempt to bypass, disable, or defeat University security technology, methods, or controls.
3. Utilize any University information resource for the purpose of scanning, infiltrating, attacking, overloading (e.g., a denial of service attack), and/or any other act intended to determine vulnerabilities, compromise, or undermine the integrity, availability, or confidentiality of any information resource, whether owned by Wentworth or not (unless part of a student academic exercise approved by faculty or by staff under the direct or indirect authorization of the CIO).
4. Take any action that obfuscates any assigned system or network identity or impersonates another system or network identity.
5. Install network or system monitoring tools (unless part of a student academic exercise approved by faculty or by staff under the direct or indirect authorization of the CIO).
6. Tap telephone or computing network communications in violation of federal or state law.
7. Access, copy, modify, or delete information stored on University owned systems without appropriate authorization.
8. Use another person's login credentials or allow others to use theirs.
9. Attempt to acquire ITR privileges for which you have not been appropriately authorized.

10. Install, run, or disseminate by any means (such as via URLs, emails, text messages, web pages, network file shares, flash drives, pagers, instant messages, voice mail, or other forms of electronic communication) software, firmware, scripts, or other digital content with malicious intent — that the individual should reasonably be expected to know is malicious — or is a nuisance (spam).
11. Store Private or Restricted University information in a digital device, system, service, or repository (i.e. a system, cloud service, or digital media), not approved by Wentworth.
12. Connect to University networks or systems from remote locations using technologies and methods not approved by DTS.
13. Configure a University *student* email account to forward messages automatically to a non-University email address for illicit purposes or without the knowledge of the account owner.
14. Configure a University *employee* email account to forward messages automatically to a non-University email address.
15. Use University ITRs in a manner that is a.) wasteful, or b.) inconsiderate of the rights of other users of ITRs, or c.) creates a hostile work environment for another employee.
16. Unauthorized disclosure of sensitive or proprietary data protected by state or federal laws and/or University policies and standards.
17. Take any action that circumvents, blocks, or disables reconnaissance on or against any ITR, as approved by the CIO.

B. Responsibilities: All ITR users **must**:

1. Use ITRs in a manner consistent with all applicable state and federal laws, such as the federal Computer Fraud and Abuse Act, and University policies and standards.
2. Avoid the risk of unauthorized disclosure of the password to any Wentworth asset by taking countermeasures, such as storing the password where it cannot be easily discovered.
3. Activate a password-protected screen saver on any Wentworth assigned computer before it is left unattended.
4. Ensure back-up copies are regularly made of University work to mitigate potential loss.
5. Scan all files and removable digital media not obtained from Wentworth with anti-virus software before connecting that media to any University computer or before accessing the file(s).
6. Store Restricted or Private University information only in approved storage locations.
7. Access, store, transfer, and grant access to all University information in a manner consistent with the *Stewardship of Information Policy*.
8. Treat the authorship of email messages as equivalent to letters sent on official University letterhead.
9. Send all official University email correspondence from an authorized University email account (i.e., an account in the "wit.edu" domain).
10. Be responsible for all information sent, received, and retained via the employee's assigned University email account.
11. Send Private or Restricted information via email only with appropriate security measures, such as public key encryption.
12. Familiarize oneself with end user cyber security best practices, e.g. how to identify a malicious email, exercising caution in responding to suspicious emails, not introducing files or storage media (flash drives, CDs, removable storage) from parties with a poor or unknown reputation, and choosing a strong password.
13. Use personally-owned computing devices to access ITRs in a manner that is consistent with the University's *Policy on Accessing University IT Resources from Personally-owned Computing Devices*.