Wentworth INSTITUTE OF TECHNOLOGY

Policy on Accessing University IT Resources from Personally-owned Computing Devices

Effective Date	Responsible Officer	Responsible Office	This Policy Applies to:
8/30/21	Vice President of Technology & Chief Information Officer	Digital Technology Services	All University departments and all faculty, staff, students, contractors, student employees, and anyone with access to University information technology resources.

1. PURPOSE

Personally-owned computing devices such as smartphones, desktop computers, tablets, and laptops, are important tools for the Wentworth community to conveniently access IT services and digital information assets. However, these computing devices may also represent a risk to the confidentiality and integrity of University information due to a lack of standard security controls. Without appropriate safeguards, personally-owned computing devices present an unacceptable risk in that they can result in compromise of the confidentiality, integrity, and availability of University information, IT assets, and services due to sub-standard security.

2. SCOPE

This policy applies to any student or employee who uses a personally-owned computing device to create, view, process, or store University information or access University technology resources.

3. POLICY STATEMENT

Wentworth permits employees to access University technology resources with personally-owned computing devices that meet the security and configuration requirements, rules, and responsibilities outlined in this policy and are used in a manner consistent with all University policies, particularly the *Information Technology Resource Acceptable Use Policy* and *Stewardship of Information Policy*. Employees who willfully disregard this policy may have their personally-owned devices blocked from accessing University technology resources.

4. DEFINITIONS

Personally-owned Computing Device	Electronic computing devices not owned or managed by the University and capable of accessing, storing, or manipulating University information, or connecting to University systems or applications, especially in an untethered manner (i.e. through a Wi-Fi connection). This Includes laptop/notebook computers, smart phones, tablets; and any other mobile computing or communications device with wireless connectivity.

5. RULES

5.1 Employees must agree to any Terms of Use or other user agreement presented when attempting to connect to the University network with their personally-owned computing device and before accessing any University technology resource.

5.2 The University reserves the right to block access to University technology asset from any personally-owned computing device that shows signs of putting University data or technology at risk or violating University policy.

5.3 The *Information Technology Acceptable Use Policy,* and any other applicable University policy, remains in effect when accessing University technology resources from any personally-owned computing device.

5.4 Employees must not download information from the University that is classified as either Private or Restricted onto their personally-owned computing device. If such information is mistakenly downloaded, it must be deleted immediately.

5.5 Employees must report suspected unauthorized access of University data via their personally-owned computing device to Technology Services immediately.

5.6 Employees must adhere to all applicable state and federal laws when using a personally-owned computing device to access University resources or store University non-Public data.

5.7 Users of University technology resources are strongly encouraged to minimally enable the following security features on their personally-owned computing device before accessing any University technology resource in order to facilitate policy compliance and lower risks to both their own and the University's data:

5.7.1 Authentication (secured with PIN, password, fingerprint, etc.)

5.7.2 Lock-screen

5.7.3 Personal computers: commercial anti-virus software installed

5.7.4 Current manufacturer operating system updates installed.

6. RELATED DOCUMENTS

Document Name	Publisher[1]
Information Technology Resource Acceptable Use Policy	WIT
Stewardship of Information Policy	WIT

7. ENFORCEMENT OF POLICY VIOLATIONS

Failure to comply with this policy may result in temporary suspension or permanent loss of privileges with respect to access to University Data and/or Information Systems.

8. EXCEPTIONS

Exceptions to this policy must receive written approval from the Chief Information Officer, with guidance from the Information Security Officer, and documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

9. REVIEW AND REVISION HISTORY

Policies must be reviewed periodically by the responsible officer or their delegate. 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 revision; if a revision, summarize the changes.

Date	Name and Title	Annual Review or Revision Summary
5/25/21	Bryce Cunningham, Information Security Officer	Finial draft produced by IT and Security Policy Working Group
7/27/21	Bryce Cunningham, Information Security Officer	Final draft vetted with IT Steering Committee, VPs, department heads, and campus community
8/25/21	Bryce Cunningham, Information Security Officer	Approved by CIO
6/7/22	Bryce Cunningham, Information Security Officer	Annual review

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