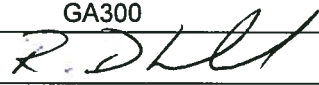


Policy #	GA300
Approved by:	
Name:	Rani Dhaliwal
Title:	Vice-president Finance and Administrative Services
Approval Date:	June 18, 2012
Policy Holder:	Vice-president Finance and Administrative Services
Administrative Contact:	Chief Information Officer
Replaces Policy Dated:	May 22, 2002
Review Date:	June 2017

Acceptable Use Policy for Technical Services

Purpose/ Rationale:

The Humber College Institute of Technology & Advanced Learning (hereafter referred to as "Humber"), in part through its "Acceptable Use Policy," seeks to achieve the following four goals:

- a) Protect students, employees, suppliers, and guests
- b) Adhere to all applicable laws and regulations
- c) Exist within the global community as a responsible citizen
- d) Maintain the integrity and quality of technical services

This document is available in alternate format on request.

Scope:

All students, employees, suppliers, and guests of Humber and the University of Guelph-Humber are required to adhere to the "Acceptable Use Policy" at all times when using any of Humber's technical services either remotely or while on campus. Examples of services covered by the "Acceptable Use Policy" include Humber's data network, desktops, Wi-Fi (wireless) network, learning management system, mobile devices, e-mail, enterprise resource planning software, telephones, printers/copiers, storage network, laptops, audio/visual equipment, and Internet links. This policy applies to both centrally managed technical services and technical services administered by Schools/Departments. Any use of any technical service, including use carried out on a privately owned computing devices not managed or maintained by Humber, is governed by the "Acceptable Use Policy."

Definitions:

Client: Any individual or entity (includes students, employees, suppliers, and guests) using one or more technical services at Humber (also known as a "user").

Data: Information in a raw or unorganized form (such as letters, numbers, symbols, or graphics) that refer to, or represent, conditions, ideas, or objects.

Employee: Any individual (not an independent business) providing value to Humber on a regular or semi-regular basis in exchange for compensation.

Guest: Any external person or entity (includes members of the public, retirees, event attendees, prospective students, alumni, advisory groups, varsity teams, etc.).

Humber: A post-secondary, educational institution in Ontario with multiple community service programs (includes the University of Guelph-Humber).

Information: Timely and accurate data organized and presented in a way that gives it meaning/relevance leading to increased understanding or reduced uncertainty.

Personal: Any activity unrelated to Humber's mission or instructional, academic, administrative, and/or research objectives (also known as a "non-Humber activity").

Service: Value (people, process, and technology) made available to employees, students, suppliers, and/or guests in support of Humber's business objectives.

Student: Any person actively enrolled in a Humber course including individuals in fully online courses and people using a Humber community service.

Supplier: An independent business providing value to Humber (also known as a "vendor", "contractor", "strategic partner", and/or "consultant").

Policy:

1. General

- 1.1. Clients are to obey the law and abide by all Humber policies, standards, and guidelines when using any of Humber's technical services.
- 1.2. All technical services are available to Clients in support of Humber's mission and are intended for academic, administrative, and research purposes.
- 1.3. Any activity that could impact the fair, safe, and productive use of technical services or negatively impact Humber's operations, assets, and/or reputation is prohibited.
- 1.4. Clients are required to conduct themselves in an appropriate, professional manner when using any of Humber's technical services.
- 1.5. Clients are accountable for all activities logged against their credentials (username and password) or electronic signature code (including all misuse or illegal activity).
- 1.6. Use of any Humber technical service implies a Client has read the "Acceptable Use Policy" and unconditionally agreed to abide by all terms and conditions at all times.
- 1.7. Questions about this policy may be directed to the Associate Vice President of Human Resources, the Dean of Students, or the Office of the Chief Information Officer.

2. Identity/Access

- 2.1. Clients are to access technical services only using the Humber credentials (username and password) assigned to them. Use of another Client's credentials is prohibited.
- 2.2. Humber usernames and passwords are personal identifiers equivalent to a signature on a document and should never be shared or disclosed to anyone at any time.
- 2.3. Concealing one's identity when accessing a technical service is prohibited. Similarly, masquerading or impersonating another individual is also prohibited.

3. Security

- 3.1. Students, employees, suppliers, and guests are required to protect all sensitive/privileged/personal data and information in their custody.
- 3.2. To guard against inadvertent/unauthorized disclosure, employees and suppliers are to encrypt sensitive/privileged/personal data and information in storage or in transit.
- 3.3. Students, employees, suppliers, and guests are to take every possible precaution at all times to ensure no other person gains knowledge of their Humber passwords.

4. Personal Use

- 4.1. Limited use of technical services for personal use is acceptable and permitted provided that use does not violate any part of the "Acceptable Use Policy".
- 4.2. The personal use of technical services may not interfere or otherwise conflict with Humber operations or incur any additional costs for Humber.
- 4.3. Clients should use caution when using services for personal use. Data created, received, and/or stored are accessible and may be accessed by Humber at any time.
- 4.4. Humber is not responsible for non-Humber privacy/confidentiality breaches. Clients are encouraged to encrypt all personal files created, received, or stored at Humber.
- 4.5. The excessive consumption (as defined by Humber) of technical resources (network bandwidth, server time, file storage space, printer paper, etc.) is prohibited.
- 4.6. Technical services, when used for personal use, are provided "as is" and without any guarantee/warranty in the form of usability, functionality, availability, or continuity.
- 4.7. At any time and without notice, Humber reserves the right to modify any technical service. Humber may also terminate services for personal use without notice.
- 4.8. Deleting electronically stored files does not assure permanent erasure. Deleted data and information may be recoverable by Humber.

5. Humber Access

At its discretion and in accordance with applicable law, Humber may access, use, and disclose the data and information of its Clients in the following circumstances:

- a) as required by Federal, Provincial, or local law enforcement agencies
- b) to carry out essential Humber business functions
- c) as required to preserve/protect public health and safety
- d) where there are reasonable grounds to believe a law has been violated
- e) to investigate a breach of Humber policy
- f) to recover business data after an employee has left the organization

Approval is required either from the Associate Vice-president of Human Resources, the Chief Information Officer, or the Vice-president of Student & Corporate Services.

6. Prohibited Activities

Unless granted an exemption¹ by the Office of the Chief Information Officer, no Client may use (or allow anyone else to use) any of Humber's technical services to:

- a) violate any law or encourage others to violate any law
- b) impede, interfere, impair, or otherwise cause harm to the activities of others
- c) monitor or scan networked resources unless authorized
- d) intrude into the networks, systems, data files, or computers of others
- e) use, access, or disclose information on co-workers, friends, or relatives
- f) edit or delete one's own student, employee, supplier, and/or guest records
- g) install, use, or distribute software for which one does not have a license
- h) access, modify, distribute, or reproduce copyrighted material without a license
- i) monitor another person's activities unless authorized
- j) create, view, collect, or share pornographic, offensive, or indecent images
- k) create or distribute malware or other disruptive/destructive constructs
- l) violate the intellectual property rights of another individual
- m) seek to learn or use another person's credentials (username or password)
- n) impersonate a person (authority delegation facilitated by software is permitted)
- o) operate a commercial or for-profit business without authorization
- p) distribute bulk mail (spam) or other messages for non-Humber purposes
- q) suggest Humber's endorsement of any political candidate or ballot initiative
- r) waste bandwidth, server time, storage space, printer paper, or other resources
- s) compromise Humber's legitimate interests

7. Privacy

7.1 All technical services – including student, employee, supplier, and guest activity – are actively monitored and logged for security, diagnostic, and audit purposes.

¹Temporary exemptions to prohibited activities may be granted by the Office of the Chief Information Officer for reasonable academic, business, and/or research purposes in consultation with the appropriate Vice-president, Vice-provost, Dean, and/or Director.

- 7.2 Humber respects the privacy of its students, employees, suppliers, and guests and will not use, access, or disclose personal data or information without cause.
- 7.3 By using a service, a Client grants Humber permission to collect, use, access, and disclose his or her personal information for “Acceptable Use Policy” purposes.
- 7.4 Employees and suppliers with access to sensitive data are required to keep such data confidential and may only use said data for official Humber business.
- 7.5 Data and information created, received, and/or stored at Humber may be accessed during the normal course of service maintenance, troubleshooting, or auditing.

8. Enforcement

- 8.1 Suspected violations of the “Acceptable Use Policy” may be reported to the Chief Information Officer or the Associate Vice President of Human Resources.
- 8.2 Pending an investigation, Humber reserves the right to immediately suspend a Client’s access to any and all technical services.
- 8.3 Employees and students who violate the “Acceptable Use Policy” may be subject to disciplinary action up to and including termination of employment or expulsion.
- 8.4 Suppliers and guests who violate the “Acceptable Use Policy” may have their Humber contracts terminated and/or be refused all future entry to Humber campuses.
- 8.5 Humber reserves the right, at its discretion, to permanently revoke student, employee, supplier, or guest access to any and all technical services at any time.
- 8.6 Clients who violate Municipal, Provincial, Federal, or International law may be subject to criminal prosecution and/or civil litigation by the appropriate authorities.

References

[Academic Employees Collective Agreement](#)
[Academic Regulations](#)
[Criminal Code of Canada](#)
[Freedom of Information & Protection of Privacy Act](#)
[Humber Code of Student Conduct](#)
[Humber Copyright Policy](#)
[Humber Human Rights Policy](#)
[Humber Occupational Health & Safety Policy](#)
[Support Staff Collective Agreement](#)

