1.0 Use of McMaster Computers and Networks

McMaster University's computing systems and networks are provided to support authorized research, instruction, administration and other intellectual pursuits consistent with McMaster University's goals and objectives. Use of these services indicates your agreement to be bound by the terms and conditions described in this document which is based on 8 previous policies.

1.1 Responsible Use of McMaster Information Technology Systems

1.1.01 Computer Access Accounts

Every McMaster faculty member, staff and registered student (undergraduate and graduate) are eligible for a unique computer access account called Mac ID that allows access to McMaster information technology resources and McMaster computer network.
Students
Mac IDs are assigned to students automatically upon registration in MUGSI. Such Mac IDs expire on an annual basis. Registered students must reactivate their Mac IDs in MUGSI at the end of each academic year.

Alumni
Once a student graduates the Mac ID will expire in January after the graduation. Alumni may choose to keep using McMaster email account (Mac ID gives access to the McMaster email account) for an annual charge.

Employees
Mac IDs for employees must be requested using the online request form. Mac IDs for employees are deleted at the end of the contract or after 13 mo. of account inactivity. Mac IDs are also deleted for those employees who are no longer employed by McMaster University.

Retirees
Once an employee retires they are entitled to a Mac ID and some of the associated services (e.g. email account) by applying for retiree access using the online form on UTS’ website. Such Mac IDs will then be valid “for life”. Any accounts that are inactive for 13 months or longer will be deleted.

Guests
Any McMaster full time employee may request a Mac ID with limited access for a guest who will be doing work for McMaster University (e.g. visiting professor/scholar, conference guests, contractor, etc.). Such IDs will be valid for duration of the guest’s stay at McMaster up to a maximum of 5 years. Such Mac IDs will then be deleted.

1.1.02 Code of Conduct

McMaster computers, networks, and telephones offer many opportunities to share information on campus and to access resources off campus. All members of the McMaster community are obligated to use these facilities in accordance with applicable laws, with McMaster standards of honesty and personal conduct, and in ways that are responsible, ethical, and professional.

McMaster computing and networking facilities and services are to be used for McMaster University purposes only and not for the benefit of private individuals or other organizations without authorization. Unauthorized access to and use of McMaster computer and network services violates this policy. Members of the University community should not take unauthorized actions to interfere with or alter the integrity of McMaster computers, networks, telephones, or the information accessed through them.
Destruction, alteration, or disclosure of data or programs belonging to others without authorization is inappropriate. Individuals should not connect unauthorized equipment to or tamper with University Technology facilities or equipment. Using any of the information technology resources of McMaster University for unethical purposes, such as harassment, is unacceptable and is subject to disciplinary actions as per McMaster University policies.

1.1.03 Central Provision of Network Infrastructure

UTS is responsible for upper-level management of the campus data network, as well as connectivity to external networks for access to:

- Internet Service providers (ISPs – currently Cogent & TiNet),
- ORION (Ontario Research and Innovation Optical Network)
- Wide-area networking (extending the campus network to nearby external sites where a McMaster staff department has relocated).

Network access is available in all buildings with data jacks typically in faculty and staff offices, as well as specific classrooms, labs and other service points, provisioned during building construction or renovation within the project budget.

Wireless access points are provided in major public spaces where students gather, in study rooms within residence buildings in conjunction with Housing, as well as classrooms in conjunction with Audio-Visual services.

Servers registered for public access from external networks must be administered according to recommendations of the IT Security Officer, and periodically scanned for compliance with good system administration practices.

- All domain names ending in ‘…mcmaster.ca’ must use McMaster IP numbers, and conversely, all machines using 130.113… IP numbers must have names within the McMaster name space (i.e. end in ‘…mcmaster.ca’).
- The only exception to this is for approved centrally supported applications hosted off-site by an external support organization. In these cases the domain name will end in 'os.mcmaster.ca'.
- If an organization with a distinct identity registers a separate domain (domain name does not end in …mcmaster.ca), that organization must contract for separate network services, including separate Internet service provision.
- It is possible for affiliated organizations requiring a distinct identity to be aliased with an existing McMaster service. For example, a multi-institutional research collaboration with equipment hosted at McMaster might request an external domain name registrar to alias the name ‘xyzresearch.ca’ to a McMaster system with an internal (unpublished) name such as ‘xyzresearch.mcmaster.ca’.
• The purpose of the McMaster data network is to facilitate the teaching, research and administrative activities of the University. The address space (130.113.0.0 through 130.113.255.255 is owned by McMaster University and may not be used without permission by any organization or entity that is not a member of the McMaster community - faculty, staff or student - for these purposes.

In cases when this policy is violated UTS will take steps to prevent traffic from the registered foreign domains from passing to/from McMaster hosts and advice to the registrar organizations involved about the improper arrangements.

1.1.04 Use of Remote Access Tools on End User Computers

UTS will ensure that currently utilized Remote Access Tools will be kept safe and secure from interference of unauthorized or improper access. UTS will only use this program when the customer authorizes its use on their computer. This program will be strictly used for troubleshooting or updating software on the customer's computer.

Before connecting to the customer's computer with the Remote Access Tool, the customer will be called by telephone.

The customer will start up the remote session and grant permission to UTS Client Services staff to proceed with the work. Once the session is over the remote interaction will be completely shut down.

1.1.05 Use of Student Computer Centres

UTS Student Computer Labs are available for student use to support their academic pursuits. Any University and Non-University affiliated areas may request a lab booking; academic instruction bookings take precedence over any other bookings.

Any activity conducted in the UTS Student Computer Labs is subject to this policy specifically section 1.1.02 – Code of Conduct.

Those individuals, areas using the Computer Centres are responsible for keeping equipment and furniture in good condition. Damages will be a responsibility of those who made the booking.

All custom software must be received by UTS minimum of 10 working days in advance of the commencement of the course. Such software must be tested by the instructor of the course minimum of 5 working days before the commencement of the course to ensure it is working properly. Instructors must provide proof of licenses if custom software is to be installed on UTS equipment.