

 <p>BRANDON UNIVERSITY Founded 1899</p>	<p>Computer Acceptable Use Policy</p>	<p><i>Approved by</i> <i>PAG (President's Advisory Group)</i></p> <p><i>Administered by</i> <i>I.T. Services</i></p>
<p><i>Administrative Policy</i></p>	<p><i>First Approved:</i> <i>January 11, 2006</i></p>	<p><i>Updated:</i></p>

Brandon University (BU) is the sole owner and operator of the BU computer system. Information Technology Services has a responsibility to maintain the system in a manner consistent with the University's mission. BU is committed to providing quality services for all faculty, students, staff, and authorized external users. The following policies have been established to ensure the security and integrity of the University's computing resources and fair and equitable access to those resources by all the members of the University community. Computing resources and networks are intended to support research, education, instruction, and administrative processes. Members of the University community using computing resources should be aware they have access to sensitive data and their computer usage on the University Network could have adverse affects on other computing facilities and users.

Scope

This policy shall apply to all University computing systems and technologies including servers, desktops, laboratory computers, network equipment, hardware, software, data, and devices related to these systems.

Violations of these policies could result in the loss of a portion of or all computing privileges and possible disciplinary action.

Authorized Use

- All faculty, staff, registered students, and authorized external guests supporting University education, research, or outreach activities are entitled access to computing resources.
- Users are allowed to use the facilities for which they are authorized.
- Users are ultimately responsible for the use of their accounts and should keep their passwords secure.
- Users are not permitted to give access by any means to other persons who do not qualify for accounts at Brandon University. Giving free resources to other persons for unauthorized purposes is prohibited.
- With the exception of e-mail access, student accounts will be disabled and removed no sooner than 180 days after the last day of class in the last session the student was registered. E-mail accounts will remain active for those students identified as Brandon University alumni for purposes of forwarding email to their personal off campus email accounts.

- Faculty and staff accounts will be removed when notified of employment termination by the appropriate dean/director. Information Technology Services will notify departments of accounts that have been inactive for at least one year.

Distribution of Resources

- The University is committed to the resources allocated for University related work. The use of the computer facilities for non work related activities that place heavy loads on University resources, cause network congestion, or that severely impact the work of others is prohibited.

Disruptive Activities

- Deliberate attempts to tamper with computing resources are prohibited.
- Any deliberate attempts to disrupt the regular operations of the University's technology resources is prohibited. Deliberate propagation of computer viruses, worms, or Trojan programs intended to disrupt normal University operations, computing resources, networks, hardware, or computer facilities is prohibited.
- Users must not attempt unauthorized access to computing installations outside of Brandon University's facilities.

Commercial Activity

- The University's computing resources are reserved for research, instructional purposes, and the professional activities of its faculty, staff, and students. The use of these systems for personal business or commercial use, such as the posting of commercial web pages and the distribution of unsolicited advertising, is prohibited.
- Users must not use accounts for private consulting or for any form of direct personal financial gain (except for appropriate contract and external accounts).

Property Rights

- Unless their owners explicitly place files in a public domain, files are to be considered private property and may not be copied, or distributed without authorization from the owner.
- Users must respect all copyrights and licenses associated with University computing facilities.
- The onus is on users/owners to familiarize themselves with their responsibilities and limitations under each software license agreement.
- Users must not attempt to:
 - Access and use software belonging to or licensed to other users or to Brandon University without proper authorization to do so;
 - Move or copy programs, or any other forms of software from one computing system to another without proper authorization. This includes personal computers, and personal workstation software; or
 - Distribute, sell, or otherwise make available software when such activity is prohibited by the license agreement for that software.

Privacy

- Users should not attempt to subvert restrictions put in place on their accounts or other accounts.
- Users should not divulge passwords to any other person. Information Technology Services does not require access to users' passwords.
- Users should change passwords for all accounts at regular intervals.
- No person shall attempt to access another user's or University files or databases without specific authorization.
- Attempts to misrepresent or use other mechanisms to access restricted data is prohibited.
- Brandon University's Student Records Policy for access to student information shall prevail in any decision pertaining to the access of student personal information and e-mail addresses. The University will publish all employee e-mail addresses on the University telephone directory unless otherwise notified by the appropriate Dean/Director.
- Users should be aware that their user accounts can and may be accessed by Information Technology Services for the purposes of system maintenance and resource management.
- The e-mail system is screened for messages that contain viruses, worms, Trojans and SPAM e-mail.

Harassment and Fraudulent Behaviour

- The sending of messages or files to another user that interfere with the legitimate work of another user, the transmission and display of abusive or obscene messages, and the sending of messages under an assumed name or modified address with the intent to misidentify the sender or origin of the message is a violation of this policy. Such activity is subject to applicable provincial and federal laws, collective agreement provisions, and University policy.

Freedom of Expression

The free exchange of ideas is central to the educational process and the **Computer Acceptable Use Policy** supports this principle. The exceptions are uses that violate the law, endanger computer resources, or violate the policies articulated in this document.