Computing Resources Acceptable Use Policy

Category: Operations; Students and Teaching

Approval: September 12, 2016

Responsibility: AVP-Information Technology

Date: October 11, 2016

Definitions:

"User(s)" are everyone who has access to any of Trent's computing and network resources. This includes both permanent and temporary employees (staff and faculty), students, alumni, contractors, agencies, consultants, suppliers, customers, guests, and business partners.

"Computing Resources" means all IT equipment (owned or managed by Trent University) that connects to the corporate network or accesses corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items.

"Network Resources" means Trent University's computing network. This includes Trent voice/data jacks, Trent's wireless network access points (eduroam and ResNet), or remote access technologies eg. VPN or SSH tunnel as maybe approved by the IT department.

"Acceptable Use" generally means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

Purpose/Reason for Policy:

This document establishes specific requirements for the use of all computing and network resources at Trent University.

The computing resources at Trent University support the educational, instructional, research, and administrative activities of the University and the use of these resources is a privilege that is extended to members of the Trent community. Users have access to valuable university resources, to sensitive data, and to internal and external networks. Consequently, it is important for users to behave in a responsible, ethical, and legal manner.

Scope of this Policy:

This policy applies to all users of computing resources and network resources as defined above.

This policy applies to technology administered in individual departments, the resources administered by central administrative departments (such as Information Technology and the University Library), personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the university's network services.

Policy Statement:

- Users may use only the computers, computer accounts, and computer files for which they have been granted authorization by the IT Department.
- Users may not use another individual's account, or attempt to capture or guess other users' passwords.
- Users are individually responsible for the appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware.
- As an authorized Trent University user of computing and network resources, users may not enable unauthorized users to access the network by using a Trent computer or a personal computer that is connected to the Trent network.
- The university is bound by its contractual and license agreements respecting certain third party resources; users are expected to comply with all agreements that they are made aware of when using such resources.
- Users should make a reasonable effort to protect their passwords and to secure computing and network resources against unauthorized use or access. Users must take reasonable steps to configure hardware and software in a way that prevents unauthorized users from accessing Trent's network and computing resources.
- Users must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- Users must comply with the policies and guidelines for any specific set of resources to which they have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
- Users must not use Trent computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.
- On Trent's network and/or computing systems, users may not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless they have been specifically authorized to do so by the Information Technology Department.
- Incidental personal use of Trent University's computing resources is acceptable provided that such use does not interfere with the user's job performance and is not a prohibited use as defined in this policy.

Fair Share of Resources:

Information Technology, and other university departments which operate and maintain computers, network systems and servers, expect to maintain an acceptable level of performance and must ensure that use of the resources by one person or a few people does not degrade performance for others. The campus network, computer clusters, servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the Trent community is explicitly forbidden.

The University may choose to set limits on any use of a computing or network resource through quotas, time limits, and other mechanisms to ensure that resources can be used by anyone who needs them. Any quotas would be determined by Information Technology and would take into consideration the available resources and the demand for such resources.

Adherence with Federal, Provincial, and Local Laws

As members of the Trent University community, users are expected to uphold local ordinances and provincial and federal law. Some Trent guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of Trent's computing and network resources users must:

- Abide by all federal, provincial, and local laws.
- Abide by all applicable copyright laws and licenses. Trent University has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.
- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.
- Not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless they have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution.

Trent University, as required by Bill C-11 and the "Notice and Notice" provision (See Appendix A), will respond to notifications of alleged copyright infringements on the University network.

Prohibited Activities

Users must utilize Trent's computing and network resources for those activities that are consistent with the educational, research and public service mission of the university.

Users are prohibited from using Trent's computing and network resources to access online gambling, view pornographic materials, conduct activities in violation of law, or in a manner otherwise precluded by University policy. For the purpose of this policy, pornographic material shall be defined as the depiction of erotic behavior (as in pictures and movies) intended to cause sexual excitement.

Prohibited activities not otherwise in violation of law may be conducted if undertaken for bona fide educational, research, or other legitimate institutional purposes.

Privacy and Personal Rights

All users of the university's network and computing resources are expected to respect the privacy and personal rights of others.

Do not access or copy another user's email, data, programs, or other files without written permission as outlined by Trent's User Electronic Information Access Policy.

Be professional and respectful when using computing systems to communicate with others; the use of computing and network resources to libel, slander, or harass any other person is not allowed and could lead to university discipline as well as legal action by those who are the recipient of these actions.

Use of the Trent University Network will be subject to the Trent University Network Connection Policy.

Access to files on university-owned computing resources will only be approved by specific personnel as outlined in the Electronic Information Access Policy. External law enforcement agencies may request access to files through valid subpoenas and other legally binding requests.

Privacy in Email

While every effort is made to ensure the privacy of Trent University email users, this may not always be possible. In addition, since employees are granted use of computing and network resources to conduct university business, there may be instances when the university, based on approval from the Associate Vice President, IT in conjunction with requests and/or approvals from senior members of the University Executive, reserves and retains the right to access and inspect stored information pertaining directly to the business of the University without the consent of the user.

Emails are not generally considered university records except when specifically communicating the business of the University: communications between a student and a university office, for example.

Rights and Responsibilities:

As a member of the University community, the university provides you with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a university employee or a registered student), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of the university that apply to appropriate use of the University's technologies and resources.

Users have the responsibility to keep up-to-date on changes in the computing environment, as published by the IT Department through the university's portal (MyTrent) or e-mail "Tech Bulletins", and to adapt to those changes as necessary.

If a user is found to be in violation of the Computing Resources Acceptable Use Policy, the University may take disciplinary action, including the restriction and possible loss of network resource privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University. Individuals are also subject to federal, provincial, and local laws governing many interactions that occur on the Internet.

These policies and laws are subject to change as provincial and federal laws develop and change.

Contact Officer:

Tariq Al-Idrissi, AVP-Information Technology

Date for Next Review:

September 12, 2018

Related Policies, Procedures & Guidelines

- User Electronic Information Access Policy
- Network Connection Policy
- Computing Privileges Policy

Policies Superseded by This Policy:

- Guidelines for the Use of Information Technology

APPENDIX 'A'

Bill C-11 and the "Notice and Notice" Provision

On June 29th, 2012, Bill C-11, the Copyright Modernization Act, received Royal Assent. While most provisions of the act were brought into force on November 7th, 2012, all remaining sections of the act were brought into force on January 2nd, 2015. Some of the provisions brought into force on January 2nd, 2015 include what has been colloquially termed the "Notice and Notice" provisions for Internet Service Providers. As defined in this act, educational institutions such as Trent University are considered to be an Internet Service Provider.

The "Notice and Notice" provision allows content owners to indirectly communicate with those who have allegedly infringed the content owner's copyright. Under this act, content providers may monitor the internet and identify internet users that are infringing their copyright. The identification of such users through an address known as an IP address will not identify the particular user in question, but will identify the Internet Service Provider where the alleged act of copying happened. It is the Internet Service Provider that may be able to identify the particular user in question.

Once an alleged copyright infringement is identified by a content owner, the content owner may choose to send an Infringement Notice to the Internet Service Provider, such as Trent University. Trent's responsibilities under the act are to;

- Make efforts to identify the alleged user associated with the infringement and forward the Infringement Notice to that user, assuming the user can be identified.
- Inform the content owner that notice has been forwarded OR that notice cannot be forwarded and why.

Trent must keep records for six months following an Infringement Notice or 12 months in the case of court proceedings.

Under this act, fines for non-commercial infringement can range from $100 to $5,000 per incident.