Regis Policy on Ethical & Appropriate Use of Information & Communication Technology[1]

Introduction

Regis College's information and communication technology (ICT) resources provide a rich array of services to the Regis College community. Ensuring the continuing utility and availability of these resources is the responsibility of our entire community. These guidelines are intended to provide a framework for the protection and effective utilization of these resources.

ICT provided for the use of employees, students, and other members of the Regis College community is the property of Regis College or the University of Toronto, and is intended to be used in a manner that is consistent with the Regis College's mission.

These guidelines apply to all of Regis College's information and communication technologies, including, hardware such as personal computers, personal digital assistants, telephones, and printing devices, as well as software and other forms of information and communication technology that exist today or may be developed in the future. The use of personally owned equipment on the University's networks is covered by these guidelines, as this also involves the use of University resources.

Additionally, these guidelines address the services provided By Regis College, ICT, including email, Internet access, departmental network services, telephone, fax, voicemail, and other technologies. Moreover, as information technology protocols, applications, utilities, and services are constantly changing, nothing in these guidelines restricts Regis College from initiating new rules or guidelines as circumstances dictate or as technology evolves.

Users of Regis College ICT are expected to limit their use to the performance of Regis College-related activities, although a reasonable allowance will be made for personal use. Whether or not an amount of personal use would be considered reasonable would depend on the particular circumstances and the applicable laws and policies. Users of Regis College ICT are required to abide by all applicable laws and policies in addition to these guidelines. Reasonable personal use does not include in any circumstances the visiting of pornographic websites, the storage or distribution of pornographic material, or the accessing, storage, or distribution of unlawful or otherwise inappropriate (within the meaning of the guidelines) information.

Users should not have an expectation of complete privacy in using Regis College or the University of Toronto's ICT and related services. The issue of privacy is discussed further within these guidelines.

Regis College and/or the University of Toronto have the authority to implement these guidelines and to monitor the usage of their services if they so choose.

There are two fundamental principles that Regis College and the University follow in determining when usage of its ICT is unacceptable. One is the quantity of resources consumed; the other, the quality of the information transmitted. The former is primarily an issue of fairness — of the equitable distribution of ICT resources; the latter is an issue of the legality and potential harmfulness of the information content, which is assessed according to the policies, codes, and external laws that govern behaviour within the University.

Fair Allocation of Resources

The University of Toronto has many facilities and services that provide ICT to users. Since the capacity of the resources is finite, there are limitations that may be imposed upon the use of specific services. Those responsible for each facility or service may establish rules governing their users; such rules can address issues peculiar to the technology involved, and may constrain the use of any resource by any user, should such constraint be deemed necessary to provide equitable sharing of the resource among all eligible users.

When a facility or service establishes rules for its users, the following principles shall be observed.

1. The use of Regis College provided ICT resources must be consistent with the academic mission of Regis College,
2. Regis College has a responsibility to make users aware of its policies, preferably at the time that access to the facility or service is granted. Where feasible, users should be required to acknowledge their agreement to abide by these rules when using the facility or service.
3. All such rules must be applied fairly and consistently to all the users governed by them.

The providers of services have the authority to implement, monitor, and apply the rules and guidelines.

Appropriate Use

[1] Since Regis College and the TST contract with the University of Toronto for ICT services, this policy draws extensively on the University of Toronto policy.

Resources: While quantitative limits on resource consumption are best set by those who manage the particular facility or service, qualitative constraints should be common across the University community and arise out of a variety of sources that are not necessarily specific to ICT. For example, a complaint about discrimination or harassment in which information technology was used as a vehicle should be dealt with as any other case of discrimination or harassment would be; the involvement of ICT does not of itself make the problem special. In this regard, these guidelines simply serve as reference to some of the relevant laws, policies, and codes that should be used to determine whether usage is appropriate, what action to take when inappropriate use is alleged or suspected and what penalties may apply for misuse.

Freedoms: The University of Toronto is committed to maintaining respect for the core values of freedom of speech, academic freedom, and freedom of research. In matters of freedom of speech versus responsible speech, it should be noted that speech using ICT is not intrinsically different from speech that does not use ICT. While the University does not censor information on its networks and servers, it will act on allegations about the distribution of unlawful material, about the use of its information technology to direct abusive, threatening, or harassing communication at any individual or about any other inappropriate use. There is further discussion in the Inappropriate Use of Information and Communication Technology section below.

When exercising free speech using the University's ICT resources, such as when posting information to a publicly accessible file or web page, personal opinions must be identified as such, so that the reader understands the author is not speaking for Regis College or the University of Toronto. However, simply identifying an opinion as personal does not exempt it from the constraints of the law or the University's policies and codes.

Privacy: The University respects the reasonable privacy of electronic files stored or distributed on its servers and networks. However, users cannot have an expectation of complete privacy when using the University's ICT. ICT resources remain the University's property, and are provided to advance the University's mission. Accordingly, the University reserves the right to examine any electronic files where the University, in its sole discretion, determines that it has reason to do so. Without limiting the University's discretion in this regard, the following represent some examples of situations in which the University may decide to examine a user's electronic files:

- During an investigation into an allegation of usage that contravenes existing laws, policies, or guidelines; or
- When complying with a Freedom of Information request for data; or
- Where necessary to carry out urgent operational requirements during an employee's absence when alternative arrangements have not been made.

It should be noted that files stored electronically have an existence that differs from paper files. While paper documents may be shredded, electronic documents may exist in multiple locations — on multiple servers and disk drives, as email attachments, and in backup tapes or disks. The act of deletion from one's own hardware does not assure permanent erasure. Users of ICT should be aware of the continuing existence of their files.

In addition to the University's broad right to examine electronic files, as set out above, some policies address the University's rights with respect to particular data. For example:

1) Student and personnel records are subject to policies regarding access to and disclosure of specified information.
2) Some facilities or services include as part of their terms of use that users' files may be read by authorized personnel. Examples include a computing facility in which instructors may be given access to certain student files for teaching purposes, or a business unit in which supervisory staff may be given access to email correspondence with customers of that unit. Where such notice is not provided, however, Regis College or the University as provider of ICT resources to advance its mission is not precluded from reviewing files, as may be reasonable in the circumstances.

Inappropriate Use

Information & Communication Technology

Users of information and communication technology may enjoy relatively unencumbered use of these services but in return they have an obligation to act responsibly and respect the rights of others. An obvious requirement is to obey the laws of Canada and Ontario, and to abide by the policies and codes of the University. These provisions deal with issues such as harassment, threatening behaviour, hate crimes, libel and defamation, discrimination, theft, fraud, and plagiarism, whether ICT is involved or not. Particular facilities and services may impose additional conditions on their users. Some specific examples of inappropriate use that might arise from the violation of laws or University policies are set out below. The list is not exhaustive.

Unauthorized Use

For students, refer to section B.5.b of the *Code of Student Conduct*, which addresses the use of computer systems for which access rights have not been granted, or using University facilities for commercial, disruptive, or malicious purpose.

For employees, refer to the policy on conflict of interest and relevant contractual and collective agreement provisions. The University is entitled to determine whether an activity is a legitimate use of the employee's time and is consistent with the employee's other obligations. If an employee is making personal use of a facility or service, the employer has the discretion to require that this activity cease, and in some cases may impose disciplinary action up to and including dismissal if a directive to cease is not complied with, or if there is other inappropriate use of ICT resources.

Other members of the University community (alumni, status-only appointees, visiting professors, postdoctoral fellow, consultants…) who are granted access to our systems also have an obligation to use ICT resources in a way that does not conflict with the interests of the University, which is providing the resources.

Authorization of Access

Access to ICT resources at the University of Toronto may only be provided by the personnel who are responsible for those systems. A person who has been given such access does not, in general, have the authority to extend that privilege to anyone else.

Individuals who have been assigned an email or computer account have a responsibility not to share their access with anyone else, even for the sake of convenience. Users should never share their passwords, nor should they permit other people, either internal or external to the organizational unit, to access or use their account by any other means.

Individuals are responsible for the actions taken under their identity. Any person who has reason to suspect that access to his or her account may have been compromised has an obligation to bring the situation promptly to the attention of the administrators of the system.

On occasion, situations may arise related to accessing voicemail and email accounts assigned to an individual where their password is required, and the person is not available to access the data or service. Since, as a guiding principle, voicemail and email passwords should not be shared, alternative approaches, such as directing auto-reply email and extended absence voicemail messages to a colleague or supervisor's email or phone number should be implemented, wherever reasonably possible.

Discrimination & Harassment

Issues of harassment based on sex and sexual orientation are covered by the *Policy and Procedures: Sexual Harassment*, whether or not ICT is involved. Issues of discrimination and discriminatory harassment, including harassment based on race and creed, are covered by the *Statement on Prohibited Discrimination and Discriminatory Harassment*, whether or not ICT is involved. Additionally, issues of harassment and discrimination are covered by the *Ontario Human Rights Code* and the *Criminal Code of Canada*.

Unsolicited correspondence (including spam) may be viewed as harassment by the recipient. The University policy on harassment, however, is concerned with comments that are directed at specific individuals because of their personal characteristics. If the correspondence is mass mailed, it should be addressed under local rules for the service used, which should prohibit or restrict unsolicited bulk mail. Users of email are advised to delete spam without opening any attachments, and to turn off the "viewing pane" in their email application so as to prevent message contents from appearing automatically.

Pornography

Using ICT resources to visit pornographic sites, or for the storage, or dissemination of pornographic material is inappropriate. Possession of child pornography is also a criminal offence.

Unauthorized Disclosure of Information

The disclosure of certain types of information is prohibited by law and/or policy, which are applicable whether or not ICT is involved. The key University policy in this area is the policy on *Access to Information and Protection of Privacy*. For student records, there is a specific policy on *Access to Official Student Academic Records*.

Copyright, Trademark, and Intellectual Property Rights Violations

Unauthorized copying of software is covered by the *Canadian Copyright Act*, and constitutes a criminal offence. The "fair use" provisions that apply to photocopies used for teaching do not apply to web pages. The Centre for Teaching Support & Innovation (CTSI) in Robarts Library can provide guidance to instructors. The use of commercial software for which a license fee is required, or the downloading and/or distribution of music or video files, for which license fees and distribution rights have not been paid or agreed upon, constitutes an infringement of Copyright, Trademark, and Intellectual property rights, and is illegal. (This is a transitory issue relative to music as a Federal Court decision is being appealed by CRIA.)

The unauthorized use of any form of device to audiotape, photograph, video-record or otherwise reproduce lectures, course notes or teaching materials provided by instructors is covered by the *Canadian Copyright Act* and is prohibited. Students must obtain prior written consent to such recording. In the case of private use by students with disabilities, the instructor's consent must not be unreasonably withheld.

In other situations where an individual photographs, audiotapes, or otherwise records activities in which she or he is taking part, without the permission of other participants, the nature of the activities must be examined. Where participants have a reasonable expectation of privacy, unauthorized recording of their activities may be unlawful. Additionally, the *Criminal Code of Canada* makes surreptitious third-party recording of conversations or other activities illegal except where there is explicit legal authority to make such recordings (e.g., phone tapping).

Plagiarism

Issues of plagiarism and misrepresentation are covered by the *Code of Behaviour on Academic Matters*, whether or not ICT is involved.

Criminal Activity

Issues of possible criminal activity, such as theft or criminal harassment or threats, are covered by statute (such as the *Criminal Code of Canada*) as well as by internal policies such as the *Code of Student Conduct*. They should be referred to the Community Safety Office and to the University Police, who can provide advice about appropriate responses and assistance with prosecution of the offence, whether or not ICT is involved.