RESPONSIBLE USE OF INFORMATION TECHNOLOGY FACILITIES AND SERVICES

THOMPSON RIVERS UNIVERSITY
805 TRU Way
Kamloops, BC V2C 0C8
tru.ca

POLICY NUMBER	BRD 16-0
APPROVAL DATE	March 27, 2020
AUTHORITY	Board of Governors
CATEGORY	Board
PRIMARY CONTACT	Vice President Administration and Finance
ADMINISTRATIVE CONTACT	(TBD)

POLICY

This policy is intended for the general support of and to provide a foundation for responsible use of Thompson Rivers University (TRU) information technology facilities and is applicable to all TRU students and employees.

TRU encourages research and scholarship to increase knowledge and understanding. It upholds academic freedom to engage in open inquiry and public discourse in an atmosphere of mutual respect. Computing and communications facilities regardless of location (including any TRU owned, leased, or cloud computing, telephone and communications services, equipment, devices and facilities) shall be used in a manner which is consistent with the requirements of TRU.

REGULATIONS

1. RESPONSIBLE USE

1.1. Computer IDs, accounts, and other communications facilities are to be used for authorized purposes. Subject to TRU Policy ADM 4-2, Conflict of Interest, limited personal use is acceptable if it does not interfere with use of the facility for its intended purpose and, in the case of employees, it does not interfere with their job performance.

1.2. Users are responsible for the uses to which their computing accounts are put. Users must not share their login credentials (username and password) to any accounts to which they have access.

1.3. Users are prohibited from accessing other users' computer IDs or accounts and communications, without specific prior authorization of the user and from the appropriate administrative head of unit.

1.4. Users must not misrepresent their identity as senders of messages nor vary the content of such messages with intent to deceive.

1.5. All users must adhere to TRU policies and all laws that govern the use of TRU's computing and communication facilities. Applicable legislation includes, but is not limited to, the Criminal Code of Canada, the B.C. Civil Rights Protection Act, the Canadian Copyright Act, the B.C. Freedom of Information and Protection of Privacy Act, and the B.C. Human Rights Code.

2. PRIVACY AND SECURITY

2.1. Users must:

a. Preserve the privacy of data to which they have access in accordance with applicable laws and the University's policies including the Information Classification Standard and Confidentiality of Student Information;

b. Respect the privacy of others by not tampering with e-mail, files, or accounts they use; and

c. Respect the integrity of computing systems and data.

For example, employees must not: intentionally use external email systems[1] for University business, develop programs or make use of already existing programs to harass other users, infiltrate a computer or computing system, damage or alter the components of a computer or computing system, gain unauthorized access to other facilities accessible via the network, or inappropriately use the telephone system.

In order to preserve the custody or control of University records, employees must: (i) not use systems or software prohibited by the University; and (ii) only use systems including email under the custody or control of the University.

2.2. Although electronic records, including log data, on TRU equipment are the property of TRU and TRU is entitled to review those records, the user community can be assured that system administrators will not examine electronic files without the individual's knowledge, except in emergencies or under circumstances where that access is required to perform their normal job functions. These include system administration, protecting the university from malware and other malicious activity, or repairing systems. In no event will ITS personnel examine other users' electronic files without authorization from the Vice-President Administration and Finance.

3. INTELLECTUAL PROPERTY

3.1. Users must respect the legal protection provided by copyright laws for computer programs and data compilations and for all other works (literary, dramatic, artistic or musical). Also, users must respect the legal protection provided by trademark

[1] Note: The *BC Freedom of Information and Protection of Privacy Act* (FIPPA) permits employees to use the same communication method used by the individual to respond to their email or other technology-based communication (such as Facebook). For example, there are no issues with TRU employees responding from a TRU email account back to an individual's Gmail account.

law and the common law for names, marks, logos, and other representations that serve to distinguish the goods or services of one person from another.

3.2. Users must respect the rights of others by complying with all TRU policies regarding intellectual property regardless of medium (i.e. paper or electronic).

4. FREEDOM OF EXPRESSION

Users should be aware that, while the University has programs to screen e-mails for viruses, worms etc., its practice is not to control the information available on our campus network.

5. HARASSMENT

All users must comply with the Respectful Workplace and Harassment Prevention Policy BRD 17-0.

6. EXAMPLES OF ILLEGAL USES

The following are representative examples only and do not comprise a comprehensive list of illegal uses:

- Uttering threats (by computer or telephone);
- Child pornography;
- Copyright infringement.

7. EXAMPLES OF UNACCEPTABLE USES

The following are representative examples only and do not comprise a comprehensive list of unacceptable uses:

- Seeking information on passwords or data belonging to another user;
- Making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others;
- Distribution of pornographic materials (provided that those with a legitimate academic purpose for doing so, may distribute such material for that legitimate academic purpose);
- Copying someone else's files, or programs, or examining such information unless authorized;
- Attempting to circumvent computer security methods or operating systems (e.g. subverting or obstructing a computer or network by introducing a worm or virus);
- Using TRU-provided computer accounts for commercial purposes such as promoting by broadcast non-educational profit-driven products or services;

- Intercepting or examining the content of messages, files, or communications in transit on a voice or data network;
- Gambling, betting, or pyramid schemes;
- Interfering with the work of other users of a network or with their host systems, seriously disrupting the network (e.g. chain letters or spamming), or engaging in any uses that result in the loss of another user's files or system; and
- Harassing or discriminatory messages.

8. SYSTEM ADMINISTRATORS

Subject to Section II(2) above, this policy shall not be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties.

Complaints under this policy may be directed to the administrative head of a unit or to the head of Information Technology Services.

9. ACTIONS

9.1. Breaches of this Policy may be subject to the full range of disciplinary and other formal actions. In addition to any other sanctions that TRU may levy in the event of a violation, TRU may withdraw computing privileges and network access.

9.2. TRU reserves the right to limit, restrict or extend computing privileges and access to its computing and communications resources, including all information stored therein.

NOTE

This Policy is not intended to set forth an exhaustive list relating to the use of TRU computing resources.

All users continue to be subject to all applicable laws and TRU policies and Information Security Standards (see TRU Policy Web site http://www.tru.ca/policy and Information Security Standards website https://www.tru.ca/its/infosecurity/standards.html).