Policy

Title	**IT Services Acceptable Use**		
Classification	Administrative	**Oversight & Responsibility**	Office of the VP & CFO; IT Services
Category	Information Management & Technology	**Effective Date**	2014 Oct 01
Approval	Executive	**Policy No**	1063

This policy is applied in a manner consistent with applicable statutory and legal obligations, including university collective agreements and terms of employment.

NOTE: The most up-to-date versions of our policies are posted on the policy & procedure website. If you've printed this policy, check the website to be sure you have the current version.

Purpose and Jurisdiction

The purpose of this policy is to define the acceptable use of Information Technology (IT) Resources in support of the mission of Royal Roads University. It builds on the principles of accountability, transparency, privacy, and fairness, to support a functional environment for work and study in which these resources are protected. This policy applies to anyone who uses or accesses any IT Resource belonging to, under the control or in the custody of, Royal Roads University.

Acceptable Use

Royal Roads University authorizes the University community to use its Information Technology resources to fulfill and advance the University's teaching, learning, research, service, administrative, and community development missions. In addition, the University permits limited personal use of these resources, provided this use does not violate any law, statute, or University policy. Users who require a private means of computing and sending electronic communications should utilize a personal device unconnected to the University's internal IT network.

The University respects the privacy of all users of its IT resources, and uses reasonable efforts to maintain confidentiality of personal information. Circumstances may arise in which such privacy cannot be maintained. Such circumstances include, but are not limited to:

1. Access to personal information may be granted to an authorized user, system administrator or agent to meet legitimate University business needs and operational requirements, or in the event that an authorized user is unavailable, or has his or her access revoked.
2. The University may audit, access or restore any IT resource within its environment when it has reasonable grounds to suspect a breach of acceptable use or a possible violation of any law or University policy.

Such access will be subject to the authorisation of the appropriate Vice-President (or designate) in consultation with the Provost.

Authorized users must exercise good judgment in determining what is acceptable use of IT resources with due regard to this policy, other University policies and community standards. Some activities may be appropriate in a specific context (e.g. for authorized academic and research purposes), while some are not appropriate in any context.

Authorised users have an obligation to take all reasonable steps (e.g. password protection and strengthening) to protect the confidentiality, integrity, and availability of IT resources and report

encountered vulnerabilities to the computer services help desk. Failure to do so may constitute a breach of this policy.

Examples of a Breach of Acceptable Use
Unless explicitly authorised, a breach of acceptable use includes, but is not limited to:
1. Allowing others to access your assigned personal Account
2. Failure to exercise reasonable care in safeguarding Accounts and information
3. Accessing someone else's personal Account
4. Seeking information on passwords or information belonging to others
5. Breaking or attempting to circumvent licensing or copyright provisions
6. Copying, deleting, intercepting, or examining someone else's files, programs, or information
7. Attempting to collect, use, or disclose, the personal Information of others
8. Using IT resources to harass or bully others
9. Attempting to circumvent information security provisions or exploit vulnerabilities
10. Using IT resources (e.g. University computing account or workstation) for unauthorized commercial purposes
11. Any interference with the ability of others to use IT resources whether it is disruptive or not
12. Falsifying or misrepresenting your identity
13. Viewing or using pornographic or offensive material in a work, study, or public location
14. Distributing or disseminating pornographic or offensive material in any location

Outcomes
If the integrity or security of an IT resource is compromised or at risk the IT Services Director or designate may direct the locking or quarantining of an Account or resource at his or her sole discretion. Upon reasonable belief by the IT Services Director that a violation of this policy may have occurred, the IT-Services Director or designate will conduct an investigation.

If access to any personal Information is required, authorisation will be requested of the appropriate Vice-President (or designate) in consultation with the Provost.

If insufficient evidence of a violation of the policy is found, the investigation will be closed and involved parties notified where appropriate.

The IT Services Director will issue a written decision regarding the alleged policy violation within a reasonable timeframe, normally 30 days. Actions noted below may be initiated upon determination of a violation of this policy. If a violation is determined to have occurred, the following actions may be initiated by the IT Services Director:

CLASS OR SEVERITY	POSSIBLE OUTCOMES
Minor violation of the AUP	Warning
Serious or repeated violation of the AUP	Escalation to appropriate authority or disciplinary process and/or restrictions on access or use
Possible violation of another University policy or regulation	Forward for investigation by applicable process under the applicable policy or regulation
Possible violation of federal, provincial, or municipal law or statute	Forward for investigation to law enforcement

This policy prohibits any use of IT resources which potentially violates any other Royal Roads University policy, code or agreement, constitutes academic or non-academic misconduct, or which violates federal, provincial, or municipal laws or regulations.

In addition to outcomes under the policy, such violations may be prosecuted under those laws and policies. Any information resulting from an investigation under the AUP may be shared for the purposes of such prosecutions.

Related Documents and Information

Related RRU policies

- Freedom of Information and Privacy
- Information Security
- IT Services Information Security Framework
- Network Access and Email Use

Review and Revision History

Date	Action
2014-Oct-01	Approved by Executive; current published version
2021-Oct-19	Transfer to new template – no content change
Next Review	
2017-Oct-01	For review