Policy

Title	**IT Resource Access and Acceptable Use**		
Classification	Administrative	**Oversight Responsibility**	Office of the Vice-President, Finance and Operations
Category	Information Management and Technology	**Responsible Office**	IT Services
Approval	Executive	**Effective Date**	2024-May-30
		Document No.	1063

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

The most up-to-date versions of the University's policies are posted on the policy and procedure website. If you've printed this policy, please check the website to ensure you have the current version.

The first appearance of terms in **Bold** in this document (except titles) are defined terms – refer to the Definitions section.

1.0 POLICY STATEMENT

Royal Roads University (University) provides access to **IT resources** for **members of the University Community** in fulfillment of the academic, research, and administrative mandates and goals of the University. The assignment of IT resources is based on a **user's** role and assigned responsibilities. The assignment structure, any changes, and any necessary revocation of IT resources follows a formal, documented process developed and implemented in consultation with IT, Human Resources, and relevant work units across the University.

2.0 SCOPE AND COMPLIANCE

This policy extends to members of the University community. Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, contract, or other relationship with the University. Allegation of a breach and any disciplinary action are managed according to legislation, regulations and University policies, standards, procedures, collective agreements, or contracts.

This policy and related policies, standards, and procedures (see Related Documents) form the foundation of the University's information, data, and IT resource security in support of the Governance policy*, Information and Data Management and Security,* and applicable legislation and regulations.

3.0 POLICY TERMS

3.1 User Accounts and Resources

a) Prior to establishment of a user account and issuance or use of IT resources, each user is required to provide written acknowledgement of agreement to comply with the University's requirements for the protection and security of information, data, and IT resources.

b) Access privileges for each user account and IT resources are role-based and may change as a result of changes to a user's role ~~and/~~or responsibilities.

3.2 IT Resource Safeguards

IT resources are provided for the purpose of carrying out University business. IT Services has established safeguards that users are expected to follow to protect the IT resources, including:

- completing IT security training programs;

- using IT resources for their intended purposes;
- avoiding unacceptable use;
- signing out of and locking unattended equipment;
- not sharing passphrases/passwords;
- ensuring personal equipment complies with IT security requirements;
- maintaining security controls at all times whether on-site or off-site; and
- having only the minimum amount of confidential, business, and/or personal information communicated or contained on equipment and only which is necessary to carry out the user's position responsibilities.

3.4 Personal Use

a) Limited personal use of IT resources is acceptable provided the use:
   - does not interfere with University business or the user's job performance;
   - is not for personal or commercial business or financial gain;
   - does not breach any law, terms of employment, contract, collective agreement, or any applicable University policy or standard including unacceptable uses set out in Appendix A.

b) Personally owned devices, including hubs, switches, routers, and wireless access points ("hot spots"), are required to connect to established remote networks and are not permitted to connect to the University's secured network.

3.5 Email Use

a) The University supports the use of email for business purposes and respects user privacy. However, email messages may be subject to monitoring, access, and disclosure (see s. 3.6). Where feasible, user consent is obtained prior to any action taken. In the event of an urgent or emergency matter for which user consent cannot be obtained, IT Services may proceed to address and resolve the matter with the approval of the Vice President, Finance and Operations.

b) Mobile devices that access a University's email account are required to have appropriate security controls, including encryption and multi-factor authentication, in place as directed by IT Services.

c) Email messages that create a business record that requires preservation are retained in accordance with the University's records retention schedule. Transitory emails are not retained, and users are required to remove such messages as soon as reasonably practical.

d) Automatic forwarding of University email to a third-party system is not permitted, except by faculty and associate faculty members who also carry out duties for another Canadian public body provided that the:
   - email account is a public sector account within Canada;
   - email system is secure and meets the University standards;
   - user returns any University business records to the University; and
   - email does not contain confidential information pertaining to the University.

e) Users are required to use their University email account to conduct University business. Use of and/or linking to external email accounts to conduct University business is not permitted. f) Users are required to contact IT Services prior to engaging in email marketing to ensure the proposed service meets the Canadian anti-spam legislation and the University's network and email requirements.

3.6 Monitoring and Reporting

a) Use of IT resources, the content of emails, information access, and other forms of electronic communication are subject to audit, monitoring, blocking, and removal of access privileges, including automated screening for malicious email and emails that contain confidential data.

b) If the integrity, safety, or security of an IT resource is at risk or compromised in an urgent or emergency matter, or there is a reasonable belief that a violation of an applicable policy has occurred, IT is permitted to investigate and seek resolution subject to applicable legislation, regulations and University policies, standards, procedures and contracts.

4.0 AUTHORITIES, ROLES AND RESPONSIBILITIES

4.1 Vice President, Finance and Operations (VPFO)

The VPFO:

a) ensures relevant policies, standards, procedures or other relevant directions are in place to protect the integrity, confidentiality, and reliable availability of IT resources used for academic and administrative purposes; and

b) acts on reported IT security issues, including informing the Executive, as appropriate.

4.2 Associate Vice President, IT Services (AVP IT)

The AVP IT:

a) oversees the management and security of University IT resources;

b) ensures appropriate acceptable use practices and procedures are in place and comply with mandated and standardized IT security directions and guidance; and

c) reports to the VPFO regarding issues related to IT security systems that have compromised or may compromise the University's IT resources.

4.3 Users

Users are responsible for taking all reasonable steps to safeguard the University's IT resources in their care and control and to report non-compliance as set out in this policy and all applicable University's policies.

5.0 DEFINITIONS

For the purposes of this policy**:**

IT resources means services, devices, and facilities owned, leased, or provided by the University and used to store, process, or transmit electronic information and/or data in virtual, remote, cloud-based, and/or physical environments, and which includes, but is not limited to:

- computers and computer facilities;
- hardware and software;
- end-user mobile and portable devices such as laptops, smartphones, tablets, desktops, and workstations;
- electronic storage media such as CDs, USB memory sticks, and portable hard drives;
- communication gateways and network equipment, including servers, and non-computing devices programmed for applications and can transmit data over the internet or other networks;
- email systems; and
- telephones and other voice systems.

Members of the University Community means members of the Board of Governors, employees, students, contractors, volunteers, guests, visitors and others who access and/or participate in University academic, administrative, and research activities and operations undertaken on behalf of the University on or off-campus.

Users means members of the University community who access and/or use the University's information technology resources and/or systems.

6.0 INTERPRETATION

Questions of interpretation or application of this policy or its procedures will be referred to the Vice President, Finance and Operations for resolution.

7.0 RELATED DOCUMENTS

Royal Roads University Documents and Information

- Appendix A –Unacceptable Uses of IT Resources
- Information and Data Management and Security (policy #1097)
- Information Technology System Security (policy #1098)
- Network Access (standard #1098-S)
- Privacy and Protection of Personal Information (policy #1090)
- Records Management (policy #1029)

Legislation and Other Information

- Canada's Anti-Spam Legislation (CASL), SC2010, c.23
- Center for Internet Security Controls (2023), v.8
- *Freedom of Information and Protection of Privacy Act*, RSBC 1966, c. 165 and applicable Regulations
- ISO 27001:2022 – Security Control Framework and Annex A

Review, Revision and Approval History

Date	Activity
2014-Oct-01	Approved by Execuitve; initial implementation and effective date
2024-May-30	Revised; approved by Executive; new effective date
2025-May-30	Next Review – (one year post-implementation)

APPENDIX A

Unacceptable Uses of IT Resources

Users are to exercise good judgment in their use of IT resources and to use the resources for the University's business. There are some activities that interfere with or disrupt the business use. Unless explicitly authorized by a user's portfolio Vice-President (or designate) and the Vice President, Finance and Operations (or designate), certain activities are unacceptable uses of the University's IT resources and are not permitted. These include, but are not limited to the following:

- access, store, download, transfer, and/or send discriminatory, illegal, threatening, harassing, pornographic, objectionable, or discriminatory material;
- violate any applicable laws;
- allow an unauthorized user to access your assigned personal account;
- knowingly access or attempt to access another user's personal account;
- failure to exercise reasonable care in safeguarding personal accounts and devices;
- unauthorized access, use, or disclosure of the University's proprietary, business, or confidential information related to students, staff, vendors, or other third parties
- infringing on or attempting to circumvent copyright, trademarks, licensing, or other legal protection provided;
- use IT resources for unauthorized commercial or personal business;
- falsify or misrepresent your identity;
- knowingly introduce a worm, malware, or virus or perpetuate a scam;
- send and/or forward non-University commercial electronic messages or chain mails;
- access gambling sites;
- attempting to bypass or tamper with IT security provisions or exploit vulnerabilities; and
- damage, alter, and/or destroy IT resources, hardware, or software without authorization.

Users engaging in an unacceptable use are subject to disciplinary action according to the University's established policies and procedures, applicable laws, legislation, collective agreement, or contract.