Acceptable Use of Technology and Information Resources Policy	
Category: Administrative	**Approval Date:** October 13, 2020
Policy Owner: Vice President Finance and Administration and Chief Financial Officer	**Effective Date:** October 13, 2020
Policy Administrator: Chief Information Officer	**Review Period:** 5 Years
Recommended by: Service Council	
Associated Documents N/A	

PURPOSE

To promote the ethical and responsible use of Red Deer Polytechnic's communication and information systems and information assets to minimize potential privacy, security, and litigation risks by

- making users aware that they bear responsibility for unacceptable use;
- protecting information assets and information systems from unauthorized access and disclosure;
- protecting information assets from inappropriate modification and loss;
- ensuring information is accessible and available to individuals with proper authorization, based on business need.

SCOPE

This policy applies to all employees, volunteers, contractors, students and any other individuals who create, access, transmit, store, or use the communication information systems and information assets owned by, in the custody of, or under the control of the Polytechnic. This policy also applies to any personally owned devices that are on the Polytechnic's networks, connected to its systems, or used to access Polytechnic data assets.

POLICY

General

1. The communication and information systems and information assets provided by the Polytechnic are property of the Polytechnic. They are intended to be used in a manner consistent with the Polytechnic's mission.
2. Individuals are responsible for the appropriate, ethical, and lawful use of the Polytechnic's systems and information.
3. The Polytechnic manages information technology resources to ensure that information assets and information systems are identified, secured, protected, and accessible throughout their life cycle.

Unacceptable Use

1. Unacceptable use of the Polytechnic's communication and information systems and information assets exposes the institution to security, privacy, and litigation risks. In order to mitigate these risks, the Polytechnic prohibits certain activities. Unacceptable use is not limited to the following examples:
    a. attempting to defeat, tamper with, or circumvent any security measures, controls, or restrictions placed on information systems;
    b. maliciously altering or destroying communication or information systems;
    c. using the Polytechnic's communication or information systems or information assets for the purpose of inappropriate communications including, but not limited to, defamation, harassment, threats, or obscenities;
    d. actions that threaten or interfere with the normal operations of information systems or that would obstruct or limit the ability of other users to use such systems. Examples include installing unapproved software, the creation of spam, phishing messages, the deliberate introduction of viruses, and using illegal torrent sites;
    e. installing, reproducing, or distributing unauthorized copyrighted material;
    f. accessing inappropriate internet subject matter or sites, such as pornography, for reasons other than instructional or research purposes.

User Responsibilities

1. All users are responsible for
    a. being aware of and complying with RDP policies and procedures relating to the use of communication and information systems and information assets;
    b. safeguarding the integrity and confidentiality of information as outlined in this and other RDP policies;
    c. creating, receiving, processing, communicating, using, and disposing of information in accordance with the Information Services policies, and procedures;
    d. taking necessary precautions to prevent unauthorized access or use of computers, storage devices, and confidential information. This includes keeping passwords confidential; and

e. using Polytechnic communication and information systems and information assets for the intended purpose.

Personal Use

1. Personal use of Polytechnic computing resources is permitted when it
   a. does not consume a significant amount of those resources or incur additional costs (e.g., excessive use of the internet bandwidth),
   b. does not interfere with the performance of the user's job or other institutional responsibilities, and
   c. is otherwise in compliance with this policy and other Polytechnic policies.
2. Further limitations may be imposed upon personal use in accordance with normal departmental procedures.

Electronic Access Control

1. Individuals require proper authorization to access information assets and information systems. The owner and/or designate of the information asset or the information system is responsible for determining permissions for access.
2. The Information Technology Services department is responsible for maintaining a roster of permissions.

Physical Access Control

1. Physical access controls are employed to protect areas containing information storage/processing facilities, information assets, and information systems.

Physical Asset Protection

1. Information assets stored in electronic form in information systems owned by, in the custody of, or under the control of the Polytechnic, are protected against storage media deterioration and software/hardware obsolescence.

Monitoring

1. System Administrators track the usage of information systems through monitoring, recording, and auditing. These duties are performed to ensure proper operation, ongoing security, information backup and resiliency.
2. The Polytechnic does not typically monitor the content of information stored and transmitted in its systems.
3. In the event of security related events or business process needs, managers and system administrators may need to review information stored or transmitted in various systems including file systems, cloud services, email, or other systems.
4. Authorized users should not consider information stored or transmitted on Polytechnic systems as completely private. If an authorized user wishes their private information to

remain completely private, they should not use Polytechnic systems to store or transmit this information.

5. As personal information for staff and students is stored on Polytechnic systems, authorized users will only collect, access, use, alter, and distribute information that is required for their Polytechnic-related responsibilities.
6. If required by their Managers, authorized users who use personal information as part of their Polytechnic-related responsibilities may be asked to sign an oath of confidentiality before being granted access to this information.

Violations

1. Individuals are held accountable for knowing and complying with Polytechnic information technology policies, guidelines, standards, and procedures.
2. Non-compliance with this policy constitutes misconduct and may be subject to penalties or discipline under Polytechnic policies or procedures and any applicable collective agreement.
3. Penalties may include termination of employment or expulsion.
4. Individuals in violation of this policy may be denied access to Polytechnic information assets or information systems and may be subject to civil, administrative or criminal action independent of any Polytechnic action, for violations of the law.

RELATED POLICIES

Intellectual Property
Student Rights and Responsibilities
Student Appeals
Student Academic Integrity and Academic Misconduct
Student Misconduct: Academic and Non-Academic
Information Access and Protection of Privacy

DEFINITIONS

Authorized User: refers to an individual who has been granted permission to access specific information systems or information.

Confidentiality: refers to restrictions on the accessibility and dissemination of information.

Communication Systems: the system for transmitting data between persons and equipment often over distance and often in the form of sound, text, or video. The system consists of physical and virtual devices, data cable, fiber, voice devices (phones, speakers), video screens and monitors, as well as the telecommunication system itself.

Information Assets: means data in any form or media that is placed into a meaningful context for users. These assets contribute to the institution's knowledge base and help to achieve strategic goals. They may be collected in relation to business, research or scholarly activity.

Information Owner: A Polytechnic employee deemed to be accountable for a particular type of information record.

Information Systems: means the infrastructure, processes, and technologies used to store, generate, manipulate, and transmit information to support the institution. Also referred to as information services or information technology.

Information Technology (IT) Resources: means all IT hardware, software, facilities, applications, and networks that are owned by, in the custody of, and operated or managed by the Polytechnic.

Integrity: refers to the reliability and authenticity of information assets. Specifically, the integrity of records refers to their trustworthiness as evidence, their ability to stand for the facts they are about, and their trustworthiness over time**.**