TITLE: COMMUNICATION AND INFORMATION SYSTEMS ACCEPTABLE USE

POLICY STATEMENT:
The communication and information systems provided by Red Deer College (RDC) are property of the College and are intended to be used in a manner consistent with the College's mission to support teaching, learning, research, administration, and service. Individuals are responsible for the appropriate, ethical, and, lawful use of RDC's communication and information systems, which is in accordance with the following applicable College policies and Canadian federal and provincial legislation:

Legislation
- Criminal Code of Canada
- Alberta Human Rights Act
- Alberta Freedom of Information and Protection of Privacy Act
- Copyright Act of Canada
- Academic Exception, as citied in Normand Tamaro, *The 2014 Annotated Copyright Act* (Toronto: Thomson Reuters, 2014), 422.

PURPOSE:
Communication and information system technologies are powerful tools for accessing and distributing information and knowledge. The purpose of this policy is to promote the ethical and responsible use of the College's communication and information systems to minimize potential privacy, security, and litigation risks to the College resulting from the unacceptable use of these systems and to make users aware that they bear the primary responsibility for any unlawful or unacceptable use.

SCOPE:
This policy applies to all employees, volunteers, contractors, students and any other individuals who create, access, or use the communication and information systems owned by, in the custody of, or under the control of RDC. This policy also applies to any personally-owned devices that are on the College's networks since they involve the use of College resources.

PRINCIPLES:
All decisions and/or actions involving RDC's communication and information systems owned by, in the custody of, or under the control of the College, are conducted in consultation with the Information Technology Department.

DEFINITIONS:
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, but may also be 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 Systems: the infrastructure, processes, and technologies used to store, generate, manipulate, and transmit information to support the College, also referred to as information services or information technology.

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

GUIDELINES:

1. Individuals using RDC's communication and information systems, use them in a way that is:
   1.1. Lawful.
   1.2. In compliance with College policies, procedures, and guidelines.
   1.3. Consistent with the purpose for which they are intended.

2. Unacceptable use of College's communication and information systems exposes the College to security, privacy, and litigation risks. In order to mitigate these risks, the following activities are prohibited. Unacceptable use is not limited to the following examples:
   2.1. Attempting to defeat, tamper with, or circumvent any security measures, controls, or restrictions placed on information systems.
   2.2. Attempting to gain unauthorized access to restricted information systems.
   2.3. Maliciously altering or destroying communication or information systems.
   2.4. Using RDC's communication or information systems for the purpose of inappropriate communications including, but not limited to, defamation, harassment, threats, or obscenities.
   2.5. Using the College's communication or information systems to promote or sell products or services for personal gain that would be in direct conflict (per the Conflicts of Interest and Conflict of Commitment Policy) to their position or obligation at RDC.
   2.6. Interfering with the normal operations of information systems that would obstruct or limit the ability of other users to use such systems. Examples include, but are not limited to, the creation of spam, the introduction of viruses, or sending multiple copies of the same or similar email to one address (mail bombing).
   2.7. Installing, reproducing, or distributing unauthorized copyrighted material.
   2.8. Installing unauthorized hardware or software.
   2.9. Accessing inappropriate internet subject matter or sites, such as pornography, for reasons other than explicit instructional or research purposes.
   2.10. Endangering RDC's information systems by making them vulnerable to potential security risks. Examples include, but are not limited to, visiting unsecure websites, such as torrent sites, clicking on unsolicited links in emails or "pop-up" advertisements on websites.

3. Users are responsible and are held accountable for:

    3.1. Being aware of and complying with College policies, procedures, and guidelines relating to the use of communication and information systems.

    3.2. Safeguarding the integrity and confidentiality of information as outlined in this and other College policies.

    3.3. Creating, receiving, processing, communicating, using, and disposing of information in accordance with the Information Services policies, procedures, and guidelines.

    3.4. Taking necessary precautions to prevent unauthorized access or use of computers, storage devices, and confidential information. This includes ensuring that personal passwords are kept confidential.

    3.5. Using the College's communication and information systems for its intended purpose, which is the performance of College-related activities. Personal use of the College's computing resources for other purposes is permitted when it does not consume a significant amount of those resources or incur additional costs (e.g., excessive use of internet bandwidth), does not interfere with the performance of the user's job or other College responsibilities, and is otherwise in compliance with this policy and other College policies. Further limits may be imposed upon personal use in accordance with normal departmental procedures.

PROCEDURE:

1. The College has the right to monitor, record, and audit the use of College systems and equipment. RDC routinely monitors network traffic.
2. If there is probable and reasonable cause to suspect illegal or unacceptable conduct, the College undertakes monitoring, recording, and auditing of an individual's information systems.
3. Any staff or faculty member notified about or otherwise aware of illegal or unacceptable use of College communication and information systems reports violations of this policy to the appropriate supervisor.
4. Violators of this policy may be denied temporary or permanent access to information systems and may be subject to penalties under College regulations, collective agreements, and provincial/federal law.
5. Users, upon logon, agree to abide by the Communication and Information Systems Acceptable Use Policy.

OFFICER RESPONSIBLE: Vice President of College Services

RECOMMENDING AUTHORITY: Service Council, upon recommendation from Deans' Council

CONSULTATION FOR REVIEW: Chief Information Officer, Deans' Council, Service Council

POLICY REVIEW DATE: January 2019

EFFECTIVE DATE: July 15, 2016

REVISION HISTORY: November 2002 (Acceptable Use of Computer and Networks Standard Practice)

January 2013 (revised and renamed Information Assets and Information Systems Acceptable Use Policy)
July 15, 2016 (revised and renamed Communication and Information Systems Acceptable Use Policy)

RELATED POLICIES:

- Academic Freedom
- Appeals: Formal
- Appeals: Informal Resolution
- Conflicts of Interest and Mandatory Disclosure
- Copyright Materials Acceptable Use
- Freedom of Information and Protection of Privacy
- Harassment and Discrimination
- Information Technology Management and Security
- Intellectual Property
- Web Site Privacy

CONNECTION TO BOARD POLICIES:

All RDC policies support relevant Board of Governors policies.