UNIVERSITY OF CALGARY

University Policy
University Procedure
Operating Standard
Guideline/Form

Acceptable Use of Electronic Resources and Information Policy

Classification Information Management
Approval Authority General Counsel
Implementation Authority Chief Information Officer
Effective Date July 23, 2019
Last Revision N/A

Table of Contents

1 Purpose 1
2 Scope 1
3 Definitions 1
4 Policy Statement 3
5 Responsibilities 6
6 Related Policies 6
7 Related Operating Standards 7
8 Related Guidelines/Forms 7
9 Related Information 7
10 History 7

1 Purpose

Electronic Resources are provided by the University to support its academic mission and facilitate the purposes of teaching, learning, research, administration and communication.

The purpose of this policy is to:

a) ensure Electronic Resources, Personal Information and Information Assets are used responsibly and lawfully; and
b) reduce the risk of loss, corruption, and mismanagement of, or unauthorized access to, Electronic Resources, Personal Information and Information Assets.

2 Scope

This policy applies to:

a) the receipt, creation, storage, handling, access, protection, transmission, disposition, use and disclosure of Personal Information and Information Assets; and to
b) all uses and users of Electronic Resources.

Note: The University acknowledges that Article 6 of the collective agreement between the Faculty Association of the University of Calgary and The Governors of the University of Calgary deals with academic freedom. Nothing in this policy is intended to limit the exercise of that academic freedom by an academic staff member or appointee.

3 Definitions

In this policy:

a) “Authorized User” means an individual who has permission to use Electronic Resources and whose identity is authenticated at the time of log-in. It includes a System Administrator.

b) “Control” means the responsibility for managing the access, handling, use and disposition of Information Assets.

c) "Custody" means the responsibility for storing Information Assets.

d) "Delegate" means an individual who has been authorized to act on behalf of another individual with respect to Electronic Resources or to access another individual's Electronic Resources accounts for administrative purposes within the scope of their duties. Delegate access may be subject to specified conditions, granted from within an application, or via the Information Technologies department and may be restricted to a specified and limited set of resources such as calendar, email and files.

e) "Electronic Resources" means the tangible and intangible assets owned, leased, or provided by the University which are used to create, receive, store, access, handle, protect, dispose of, or transmit electronic information including Information Assets and Personal Information. Electronic Resources enable all forms of electronic communications, including but not limited to email, voicemail, text messaging and website browsing through connected computer systems or the internet. Electronic Resources include computers, Mobile Computing Devices, Mobile Storage Devices, servers, software, hardware, shared drives, systems, WIFI and other networks, and related equipment, facilities and infrastructure.

f) "Graduate Students' Association" means the Graduate Students' Association of the University of Calgary.

g) "Information Assets" means information in the Custody or under the Control of the University, in any format or media, which relates to University's administrative functions, including its services, operations, finances, transactions, facilities, and Student records, or to teaching, scholarly, research or clinical activities.

h) "Information Security Classification Standard" means the University's information security standard, OSP IM010, as amended.

i) "Log" means an electronic record of events that have occurred within Electronic Resources. Logs include metadata about the events which may include time stamps, event descriptions, account information, name of sender and recipient and other data.

j) "Manager" means: (i) for the President of the University, the chair of the University's Board of Governors; and (ii) for an academic staff member, appointee, postdoctoral scholar or other employee of the University (other than the President), the SLT Member who has management responsibility for the faculty, department or unit of which the academic staff member, appointee, postdoctoral scholar or other employee is a member, or the SLT Member's Delegate.

k) "Mobile Computing Devices" means portable electronic devices including notebook computers, laptops, tablets, portable digital assistants (PDAs), "smart" phones, and other similar devices.

l) "Mobile Storage Devices" means portable devices used to store data including external hard drives, USB drives, memory cards, flash and other data storage drives, optical storage devices (e.g. CDs, DVDs, Blu-Ray disks), and other similar devices.

m) "Personal Information" means recorded information about an identifiable individual including but not limited to an individual's:

   i. name, address or telephone number;
   ii. race, national or ethnic origin, colour or religious or political beliefs or associations;

iii. age, sex, marital status or family status;
iv. employee or Student number;
v. educational, financial, employment or criminal history; and
vi. health and health care history.

n) "SLT Member" means an employee who, at the relevant time, is designated as a member of the Senior Leadership Team.

o) "Student" means an individual who is registered in a University course or program of study.

p) "Students' Union" means the University of Calgary Students' Union.

q) "System Administrator" means an individual who has been authorized to access, configure, install, secure, maintain or support Electronic Resources.

r) "University" means the University of Calgary.

4 Policy Statement

Acceptable Use

4.1 Electronic Resources may only be used by Authorized Users for University-related purposes and activities or pursuant to section 4.3.

4.2 At all times, individuals have a responsibility to use Electronic Resources, Personal Information and Information Assets for the purposes for which they were intended, and in accordance with University policies, procedures, employment agreements and collective agreements and all laws.

Personal Use

4.3 It is recognized that some personal use of Electronic Resources may occur on an occasional and limited basis provided such use does not:

a) interfere with the Authorized User's work performance;
b) interfere with any other Authorized User's work performance;
c) burden the University with incremental costs;
d) have undue impact on the operation of Electronic Resources;
e) compromise the work or reputation of the University; or
f) breach any other provision of this policy, any other University policy, procedure, employment agreement or collective agreement or any law.

Researchers' Confidentiality Obligations

4.4 The University respects researchers' confidentiality obligations as set out in their research agreements, in the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans and in any directives provided to them by Research Ethics Boards.

Safeguarding Electronic Resources

4.5 Authorized Users who are University employees must use credentials (such as passwords and multi-factor authentication) to access Electronic Resources that meet the security, authentication and complexity requirements established from time to time by the Information Technology department. Authorized Users are responsible for safeguarding and protecting the confidentiality of their credentials.

4.6 System Administrators may monitor, record and audit the use of Electronic Resources and may review Logs at any time:

a) for network maintenance purposes, including diagnosing and resolving problems;
b) for security purposes, including preventing, detecting and managing security breaches;
c) to manage and ensure the effective operation of the Electronic Resources;
d) for routine backup of data and information.

4.7 The University does not routinely monitor the content of information transmitted or stored within Electronic Resources. Managers and System Administrators may only review the contents of Electronic Resources, electronic communications and Authorized User accounts in the following circumstances:

a) with the consent of the Authorized User; or
b) if authorized by General Counsel or their Delegate and then only:
    i. if an Authorized User is on a leave of absence or has ceased employment and access is necessary to sustain the routine operation of the Manager's faculty, department or unit; or
    ii. if necessary for a purpose set out in s.4.6; or
    iii. to investigate an allegation of a breach of any University policy, procedure, employment agreement or collective agreement or any law; or
    iv. when access is required, permitted or authorized under law.

Consequently, Authorized Users should never consider their use of Electronic Resources to be completely private, including their use of Electronic Resources for electronic communications, browsing websites, creating, accessing, protecting, handling, altering or disposing of images or other electronic information or any other use whatsoever. To the extent that Authorized Users wish their personal activities to remain completely private, they must not use the University's Electronic Resources for such activities.

4.8 Managers shall refer questions regarding appropriate access and disclosure related to an Authorized User's accounts to the Freedom of Information and Protection of Privacy Act (FOIP) Coordinator.

4.9 A System Administrator or Manager may only access an Authorized User's account in accordance with sections 4.6 or 4.7. Any System Administrator or Manager who accesses an Authorized User's account other than in accordance with sections 4.6 or 4.7 may be subject to disciplinary action up to and including termination of employment. Disciplinary action will be taken in accordance with the provisions of any applicable collective agreement.

Unacceptable Use

4.10 Authorized Users shall not use Electronic Resources to create or distribute:

a) commercial or advertising material unless such material is related to their University responsibilities or, if they are a Student, unless such material is related to their University responsibilities or their responsibilities as a member of the Students' Union Legislative Council, the Graduate Representative Council (the policy making body of the Graduate Student's Association), or a student club or

organization sanctioned by the Students' Union or Graduate Students' Association; or

b) messages that are anonymous or deliberately forged or that have deceptive address header information; or

c) material that would not comply with any University policy, procedure, employment agreement or collective agreement or any law.

4.11 Using Electronic Resources, Personal Information or Information Assets inappropriately exposes the University to a number of security, privacy, litigation and other risks. In order to mitigate these risks, the following activities are prohibited:

a) attempting to defeat or circumvent any security measures, controls, or record-keeping systems;

b) attempting to gain unauthorized access to areas or files;

c) tampering with any protections or restrictions placed on Personal Information, Information Assets or Electronic Resources;

d) intentionally introducing or propagating any malicious code, "virus" or software designed to damage, infiltrate, or otherwise hinder the performance of Electronic Resources;

e) accessing Electronic Resources using another Authorized User's account, unless authorized as a Delegate or pursuant to this policy;

f) using Electronic Resources in a manner that, directly or indirectly, interferes with the rights of Authorized Users or deprives Authorized Users of the ability to use the Electronic Resources in accordance with this policy.

4.12 Electronic communication is an inherently insecure means of communication. An Authorized User will ensure that the contents of a message are secured in accordance with the Information Security Classification Standard when using Electronic Resources to distribute Information Assets to an address that is external to the University.

Personal Information

4.13 Authorized Users will create, access, use, collect or alter Personal Information using Electronic Resources only if it is necessary for a purpose related to the Authorized User's University responsibilities, and shall create, access, use, collect or alter only the amount of Personal Information that is essential to carry out the intended purpose.

4.14 Authorized Users who have access to Electronic Resources will not disclose Personal Information in Electronic Resources to anyone other than Authorized Users who need the Personal Information for a purpose related to their University responsibilities or as permitted or required by law and will only disclose the amount of Personal Information that is necessary for such purpose.

Training and Oath of Confidentiality

4.15 If required by their Managers, Authorized Users who use Electronic Resources to access Personal Information for a purpose related to their employment responsibilities will:

a) attend privacy awareness training before they are granted such access. They will also attend privacy awareness update sessions as required by the Freedom of Information and Protection of Privacy Act (FOIP) Coordinator; or

b) will sign an oath of confidentiality before they are granted such access, and will attend privacy awareness training and privacy awareness update sessions as required by the Freedom of Information and Protection of Privacy Act (FOIP) Coordinator. The oath of confidentiality will substantiate their acknowledgment that they have read and understood this policy and that they agree to abide by its terms. The applicable University faculty, department or unit is responsible for obtaining the signed oath and forwarding it to the Human Resources department which will retain the signed oath in the Authorized User's personnel file.

Intellectual Property

4.16 Nothing in this policy affects intellectual property rights as described in the Intellectual Property Policy.

Non-Compliance with the Policy

4.17 Allegations that academic staff members or other employees may not be complying with this policy may be reported to their Manager, direct supervisor or the Protected Disclosure Advisor. Allegations that Students may not be complying with this policy may be reported to the Student Conduct Office.

4.18 Individuals who do not comply with this policy may be denied access to Electronic Resources and may also be subject to penalties or discipline under University policies, procedures, any relevant employment agreement or collective agreement, and under law. Disciplinary action will be taken in accordance with the provisions of any applicable collective agreement.

5 Responsibilities

5.1 The Implementation Authority will:

a) promote and support the acceptable use of Electronic Resources and Information Assets;
b) monitor implementation and administration of this policy.

5.2 Authorized Users will:

a) be familiar with this policy and act in accordance with it;
b) attend privacy awareness training as required under this policy.

5.3 Managers will:

a) ensure that members of the faculty, department or unit for which the Manager has management responsibility:
   i. have an appropriate level of access to Personal Information in Electronic Resources, if required to perform their employment responsibilities;
   ii. are encouraged and permitted to attend privacy awareness sessions as required under this policy;
b) ensure that the faculty, department or unit for which the Manager has management responsibility obtains a signed oath of confidentiality and forwards it to the Human Resources department as required by section 4.15.

6 Related Policies

Information Asset Management Policy
Acceptable Use of Material Protected by Copyright Policy
Intellectual Property Policy

7	**Related Operating Standards**	Information Security Classification Standard Storage of Business Information Assets Standard
8	**Related Guidelines/Forms**	Request to Access a Network Account without Consent Form Oath of Confidentiality Form Dealing with Confidential Records Guide
9	**Related Information**	Commitment to the Acceptable Use of D2L

10 History

July 23, 2019	Effective. This Policy replaces the Electronic Communications Policy (2009), Acceptable Use of Information Assets Policy (2006, revised 2007), and Acceptable Use of Personal Information in Enterprise Information Systems Policy (2006, revised 2007).
January 1, 2020	Editorial Revision. Updated format and links.