University of Victoria

University Policy No.: IM7200
Classification: Information Management
Approving Authority: Vice-President Finance and Operations
Effective Date: March 2018
Supersedes: June 2012
Last Editorial Change:
Mandated Review: March 2025

ACCEPTABLE USE OF ELECTRONIC INFORMATION RESOURCES

Associated Procedures:
Procedures Regarding the Use of Broadcast Email and Other Mass Communications
Procedures Regarding the Deprovisioning of Email for Former Employees in Academic and Administrative Positions

---

PURPOSE

1.00 The purpose of this policy, in conjunction with other applicable policies, is to:

(a) set forth the acceptable use of all Electronic Information Resources in the custody or under the control of the university; and

(b) describe the rights and responsibilities of the university and of the University Community with respect to the use of these resources.

DEFINITIONS

2.00 **Administrative Authority** means individuals with administrative responsibility for units (e.g., Vice-Presidents, Chief Information Officer, Executive Directors, Deans, Chairs, Directors and other unit heads) and individuals with functional stewardship of Electronic Information Resources.

3.00 **Information System** means the people, processes, organization, technologies, equipment and facilities that collect, process, store, display, transmit, and disseminate information.

4.00 **Unit** means a group of Users, linked by a common interest or purpose, including but not limited to: faculties, departments, divisions, schools and centres.

5.00 **User** means any individual or Unit that uses or accesses Electronic Information Resources as authorized by an Administrative Authority.

6.00 **Provider** means individuals who design, manage, and operate Electronic Information Resources (e.g., project managers, system designers, application programmers, or system administrators).

7.00 **Electronic Information Resources** means devices, assets and infrastructure owned by, explicitly controlled by, or in the custody of the University including but not limited

to data, records, electronic services, network services, software, computers, laptops, tablets, smartphones, mobile computing devices, and Information Systems.

8.00 **University Community** members include

- all employees and registered students of the university;
- any person holding a university appointment whether or not that person is an employee;
- post-doctoral fellows;
- separately incorporated organizations operating on campus;
- organizations and individuals required by contract to comply with university policies and procedures;
- members of the Board of Governors;
- anyone residing on campus; and
- all other Users granted access to Electronic Information Resources

9.00 **Information Security Incident** means any adverse event whereby some aspect of information security could be threatened, including but not limited to: loss of data or records confidentiality, disruption of data or system integrity, or disruption or denial of availability.

SCOPE

10.00 This policy applies to all University Community members. It applies to all Electronic Information Resources in the custody or under the control of the University regardless of physical location.

POLICY

11.00 The university provides Electronic Information Resources to the members of the University Community primarily to serve the educational, research, and administrative purposes of the University.

12.00 Appropriate use of Electronic Information Resources is governed by the following principles:

12.01 Each User of Electronic Information Resources bears primary responsibility for their use of these services and for the information they transmit, receive, or store through use of these services.

12.02 Users are expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.

12.03 Users shall comply with all applicable laws, regulations, and contracts and are expected to behave in a manner consistent with the University's policies and mission.

12.04 Incidental use of Electronic Information Resources for personal use is acceptable but is limited to responsible activities that minimize the disruption of university business while attending to necessary personal affairs. The university is not responsible for any personal data stored on university

Electronic Information Resources as a result of incidental personal use ("personal data"):

(a) While the University takes reasonable measures to back up information and protect it from loss, the University cannot guarantee that personal data will be retained in university information systems or remain confidential. To protect their personal data from inadvertent access, disclosure or destruction, Users are encouraged to store them separately from university information systems and back them up on a regular basis. Where Users intermingle personal data with UVic Electronic Information Resources, they increase the risk that the university will unintentionally access the personal data in the course of accessing UVic Electronic Information Resources for University Business purposes.

(b) Users should understand that the university routinely monitors network patterns such as source/destination, address/port, flags, packet size, packet rate, and other indicia of traffic on UVic information systems. University system administrators and other technical transmission personnel also perform routine maintenance of UVic information systems. This routine monitoring and maintenance may unintentionally reveal personal data.

(c) As part of the university's response to an Information Security Incident, the university may temporarily expand the scope of routine monitoring activities to include computers, servers, and devices connected to the university network to look for the presence of malicious software and indications that unauthorized access to data has occurred or is occurring.

12.05 Use of Electronic Information Resources for commercial purposes is limited by University policies governing commercial activities sponsored by the University, for the purpose of enhancing the University's mission.

12.06 Connection of privately owned computer equipment to University communications services is permitted. Access to Electronic Information Resources from these computers, or from computers attached to remote networks, is also permitted. All such usage is governed by this policy. Connection of privately owned communications equipment with the intention of extending communications capabilities to other computers or communications equipment requires specific authorization of the Chief Information Officer (or designate).

12.07 Users from federated or trusted affiliates are expected to abide by this policy. Likewise, members of the University Community are expected to abide by the requisite policies at federated or trusted affiliates when using Electronic Information Resources of those affiliates.

12.08 An email or other record created using Electronic Information Resources or university Information Systems may be a university record for the purpose of the *Freedom of Information and Protection of Privacy Act.*

12.09 University Electronic Information Resources, such as a university email account and @uvic.ca email address, are provided to employees in academic and administrative positions for the purposes of conducting university business and will be deprovisioned or reassigned in accordance with the Procedures Regarding the Deprovisioning of Email for Former Employees in Academic and Administrative Positions. Supervisors may also request the removal of an employee's access to Electronic Information Resources during an employee's extended absence.

13.00 As a condition of access to Electronic Information Resources, a User agrees not to use these resources for inappropriate or unauthorized purposes. Some examples of inappropriate use include but are not limited to:

(a) Compromising or attempting to compromise the integrity of any Electronic Information Resources;
(b) Using accounts or identification numbers without authorization from the service Provider;
(c) Revealing, sharing, or showing passwords, access codes, or passphrases for accounts associated with individual Users;
(d) Sending communications that attempt to hide the identity of the sender or represent the sender as someone else;
(e) Seeking, by any means, copies of or information regarding passwords, data, or programs of another user unless explicitly authorized to do so by that user;
(f) Sending communication or using Electronic Information Resources, including email, web pages, that discriminate against or harass, defame, offend, or threaten;
(g) Using a Electronic Information Resource for non-University projects except as allowed by 12.05;
(h) Using a Electronic Information Resource for commercial or other external purposes except as allowed by 12.05;
(i) Attempting to disrupt, degrade, or interfere with the regular operation of any Electronic Information Resource;
(j) Making or using illegal copies of copyrighted materials or software, storing such copies on Electronic Information Systems, or transmitting them over University networks;
(k) Displaying or transmitting information that violates laws (e.g., copyright, criminal code, privacy);
(l) Monitoring Electronic Information Resources without authorization;
(m) Introducing or propagating any malicious or unwanted software designed to self-replicate, damage, infiltrate, or otherwise hinder the performance of any Electronic Information Resource;
(n) Initiating mass email transmissions, or other electronic mass communications:
    (i) without authorization from the University Secretary, except as set out in the Procedures Regarding The Use of Broadcast Email and Other Mass Communications; or
    (ii) to listservs, forums, discussion boards, social media sites, or other venues, provided either by the University or third parties, that segments of the University community have knowingly joined.

14.00 Any exception to the provisions set out in section 13.00 must have the prior written approval of the appropriate Vice-President (or designate), unless otherwise provided for in other University policies.

Compliance

15.00 Use of Electronic Information Resources acknowledges acceptance of and compliance with this policy.

16.00 University Systems will investigate suspected violations of this policy; recommend or implement corrective action; suspend, disable, terminate, or remove access to or from Electronic Information Resources; or take other action in accordance with collective agreements, the Framework Agreement and university policies and procedures.

16.01 The Information Security Officer, if warranted, will assemble a response team that includes the following individuals (or their designates):

- the Information Security Officer
- the Chief Information Officer
- the Administrative Authority responsible for the Electronic Information or Information systems involved.

16.02 Based on the nature of the Incident, the response team may also include the following individuals (or their designates):

- the University Secretary
- the Chief Privacy Officer
- the Associate Vice-President Human Resources
- General Counsel
- Associate Vice-President Faculty Relations and Academic Administration
- the Executive Director, UVic Communications + Marketing,
- Director, Campus Security
- Manager, Computer Help Desk
- Other Administrative Authorities
- Other subject matter experts

16.03 In cases where action will have a substantial, negative effect on a Unit or person to fulfill their responsibilities, the approval of the appropriate Vice-President (or designate) will be required before taking this step.

AUTHORITIES AND OFFICERS

The authorities and officers for this policy are:

i. Approving Authority: Vice-President, Finance and Operations
ii. Designated Executive Officer: Vice-President, Finance and Operations
iii. Procedural Authority: Vice-President, Finance and Operations
iv. Procedural Officer: Chief Information Officer

RELEVANT LEGISLATION

University Act
Freedom of Information and Protection of Privacy Act
Criminal Code of Canada

RELATED POLICIES AND DOCUMENTS

Information Security Policy and related procedures IM7800
Protection of Privacy Policy and related procedures GV0235
Records Management Policy and related procedures IM7700
Discrimination and Harassment Policy GV0205
Resolution of Non-Academic Misconduct Allegations AC1300
Licenses governing the use of computer programs and documents of all kinds.

University of Victoria

PROCEDURES REGARDING THE USE OF BROADCAST EMAIL AND OTHER MASS COMMUNCIATIONS

Procedural Authority: Vice-President, Finance and Operations
Procedural Officer: Chief Information Officer

Effective Date: March 2018
Supersedes: March 2016
Last Editorial Change:

Parent Policy:
Acceptable Use of Electronic Information Resources (IM7200)

PURPOSE

1.00 The purpose of this document is to set out procedures to be followed when sending broadcast email or other mass communications to the University Community.

DEFINITIONS

2.00 The definitions contained within the university's Acceptable Use of Electronic Information Resources apply to these procedures.

PROCEDURES

3.00 Broadcast email or other mass communications to all faculty, staff and/or students, or major segments thereof, or to other major segments of the University Community are permitted if the message is institutional in nature or relates to the critical operation of the university, and if permission has been granted by the Executive Director, Communications + Marketing (or Designate).

Exceptions to this include:

3.01 Messages for all students or specific student segments pertaining to critical academic business, or university-wide deadlines or schedules may only be sent by or with permission from the Registrar (or designate).

3.02 Messages regarding the governance of the university, including elections or ratifications required by the University Act or another university policy may only be sent by or with permission from the University Secretary (or designate).

3.03 Messages regarding issues of specific interest to faculty and librarians or a segment thereof may be sent by the Vice-President Academic and Provost.

4.00 Whenever possible, offices granted the above exception will endeavour to provide the Executive Director, University Communications + Marketing with advance notice of broadcast emails sent from their offices.

5.00 Messages from the University of Victoria Students' Society or the Graduate Students' Society to their members may be sent with permission from the University Secretary.

6.00 Under the authority of the Chief Information Officer, system outage messages may be sent to users of the affected systems.

RELATED POLICIES AND DOCUMENTS

Acceptable Use of Electronic Information Resources

University of Victoria

PROCEDURES REGARDING THE DEPROVISIONING OF EMAIL FOR FORMER EMPLOYEES IN ACADEMIC AND ADMINISTRATIVE POSITIONS

Procedural Authority: Vice-President, Finance and Operations
Procedural Officer: Chief Information Officer

Effective Date: March 2018
Supersedes: New
Last Editorial Change:

Parent Policy:
Acceptable Use of Electronic Information Resources (IM7200)

PURPOSE

1.00 The purpose of this document is to set out procedures to be followed for all employees within academic and administrative units with a university email account and mailbox when the employee leaves the university.

DEFINITIONS

2.00 The definitions contained within the university's Acceptable Use of Electronic Information Resources apply to these procedures.

3.00 University Email Account: An email account associated with the Primary NetLink-ID of an employee and used only by that employee. University email accounts are provided for conducting university business; the mailbox and contents of a university email account always remain the property of the university.

4.00 Role Based Email Account: An email account that is owned by a unit, associated with a role or position that may be monitored by multiple employees. Role Based email accounts are provided for conducting university business; the mailbox and contents of a university email account always remain the property of the university.

4.01 Role Based email accounts will be provided according to the following criteria:

- Used to support a specific role, function or service
- Used to correspond with an external entity that requires the use of a single email address on behalf of the university
- May be monitored by multiple employees, who may change, at any given time

SCOPE

5.00 These procedures only apply to University of Victoria employees who are not members of the University of Victoria Faculty Association. These procedures do not apply to members of the University of Victoria Faculty Association.

PROCEDURES

University Email Accounts

6.00 The employee's supervisor will submit a request to the Computer Help Desk indicating the departing employee's University email account address and last day of work and whether the supervisor requires access to the contents of the mailbox after the employee's departure.

7.00 The Computer Help Desk will disable the employee's University email account on the first business day after the employee's last day of employment.

7.01 If the employee has other roles at the university, such as a student or Faculty Member, the Computer Help Desk will inform the supervisor that the employee's University email account cannot be disabled.

7.02 If requested by the supervisor, the Computer Help Desk will provide instructions on how to access the contents of the mailbox prior to it being disabled.

7.03 Once an account is disabled, any email sent to it will be rejected. If this will cause an operational issue, the supervisor may request that mail sent to the account be redirected to another account for up to 3 months.

Role Based Email Accounts

8.00 The employee's supervisor will submit a request to the Computer Help Desk indicating what role based email accounts the employee departing the role had access to and whether any other employees need access to these accounts after the departing employee's departure.

9.00 The Computer Help Desk will remove the departing employee's access to the role based email account on the first business day after the employee's last day in the role and will recommend the supervisor have the password for the account be changed.

9.01 If requested by the supervisor, the Computer Help Desk will add access for any other employees who require access to the role based email account or provide instructions on how to add additional delegates to a role based email account using the self-service tool.

RELATED POLICIES AND DOCUMENTS

Acceptable Use of Electronic Information Resources