Title	Use of Information Technology Resources
Policy Area	Operations – College Systems and Resources
Policy Number *(to be assigned by Information Services)*	E.5.1
See also *(related policies)*	Protection of Privacy Policy Social Media Policy

Effective Date of Policy:	November 27, 2015
Approval Date:	November 26, 2015
Applies to:	All employees and students within the Okanagan College community and others who have been granted the use of Okanagan College's information resources.
Approving Body:	President
Supersedes:	OC Board June 28, 2005, Use of Information Technology Resources Policy April 20, 2010; Revised June 28, 2013
Authority	*College and Institute Act, Freedom of Information and Protection of Privacy Act*

The following are responsible for the administration of this policy,

Primary Office	**Contact**
Information Services	Director, Information Technology Services

Policy Statement

1.0 Okanagan College makes computers, communication devices, e-mail, learning management systems (LMS), intranet and internet resources (collectively the "Information Resources") available to authorized users to assist them in performing their work, conducting Okanagan College business and completing their educational studies. Use of these Information Resources for any purpose that is not specifically related to these purposes is prohibited, except for incidental personal use as defined in this policy.

2.0 Because Okanagan College is a public body governed by the *Freedom of Information and Protection of Privacy Act* ("Act"), records created by using its Information Resources are records within the custody or control of Okanagan

College. All users should be aware that records created and stored on the College's Information Resources may be accessible under the Act.

Scope of this Policy

3.0 This policy applies to all employees and students within the Okanagan College community and to others who have been granted the use of Okanagan College's Information Resources.

4.0 This policy refers to all Information Resources within Okanagan College whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated or contracted by Okanagan College including computers, communication devices, digital storage devices, networks and associated peripherals, software, intranet and internet and all individuals accessing Okanagan College's computing systems.

Rules and Responsibilities

5.0 All users of Okanagan College Information Technology Resources must:

5.1 comply with all applicable laws including the *Criminal Code of Canada*, *Copyright Act*, *BC Freedom of Information and Protection of Privacy Act*, *BC Civil Rights Protection Act* and *BC Human Rights Code*, and Okanagan College policies in the course of using Okanagan College Information Resources, and by licences governing the use of computer programs, software and documents;

5.2 take appropriate steps to ensure the security of Okanagan College's Information Resources by adhering to all applicable security measures including using and safeguarding all necessary passwords, and using encryption on portable storage devices;

5.3 use complex passwords and avoid using common sequences (e.g. 12345) or readily identified information (e.g. name, address, phone number, spouse's name, etc.);

5.4 secure their workstations when they are absent from them;

5.5 use only computer IDs or accounts and communication facilities which they are duly authorized to use, and use them for the purposes for which they were intended; and

5.6 respect copyrights, software licences, intellectual property rights and contractual agreements.

Prohibited Activities

6.0 The following activities are strictly prohibited:

6.1 using Information Resources to access, create, view, listen to, store or transmit material that is harassing, obscene, abusive, illegal, pornographic, discriminatory or that otherwise violates applicable laws, Okanagan College's agreements, policies or community standards, except if such use is part of assigned Okanagan College duties or course work;

6.2 tampering with files, digital storage media, passwords, or accounts of others, misrepresenting one's identity as a sender of messages or the content of such messages or attempting to circumvent or subvert security measures;

6.3 intentionally developing programs or making use of existing programs that harass other users, or infiltrate a computer or computing system, or damage or alter the software components of a computer or computing system, or gain unauthorized access to other facilities accessible via the network;

6.4 using Information Resources, services or facilities for non-Okanagan College purposes, projects, commercial or other external purposes except as described below;

6.5 unauthorized release of private/personal and/or confidential information related to Okanagan College's business, employees or students;

6.6 downloading and/or installing unauthorized programs, files or software; and

6.7 creating, transmitting, distributing, forwarding, downloading or storing any software, files or programs that infringe any copyright, trademark or intellectual property rights or which exposes Okanagan College to unauthorized legal obligations or liability.

Incidental personal use

7.0 The primary use of Okanagan College's Information Resources must be related to Okanagan College's educational and research mission, business and functions. Incidental personal use of the College's Information Resources is permitted provided that such use meets each of the following criteria:

7.1 it complies with this Policy;

7.2 it does not cause Okanagan College to incur any unauthorized cost;

7.3 it does not expose Okanagan College to risk;

7.4 it is not part of an unauthorized activity; and

7.5 it is not for commercial or personal profit of the user or for the profit of others.

8.0 Use of Information Resources for commercial or profit related purposes is restricted to those activities sponsored and authorized by a Vice President.

9.0 The foregoing sections are not intended to be an exhaustive list of permissions and prohibitions governing the use of Okanagan College Information Resources. All users continue to be subject to all applicable laws and Okanagan College policies.

Monitoring and Privacy

10.0 Okanagan College has a responsibility to ensure that all email, communications and information downloaded on or viewed from Okanagan College's Information Resources comply with Okanagan College policies, agreements and applicable laws.

11.0 Okanagan College does not regularly monitor users' use of Information Resources. However, monitoring may occur for legitimate reasons. As a result, users should not expect privacy when using Okanagan College Information Resources.

12.0 Information Technology Services staff routinely analyze network activity and logs for the purpose of troubleshooting, monitoring and addressing network security and performance and addressing system maintenance needs.

13.0 Subject to the provisions of any collective agreements between the College and its unions, including notice provisions, an employee's use of LMS may be reviewed by an employee's supervisor (Associate Dean, Dean or Director), for the purposes of employee evaluation.

14.0 Students' use of LMS may be inspected or monitored from time to time by an Associate Dean, Dean or Director, or their designate, without notice or approval for the purpose of evaluation of student compliance with College academic policies.

15.0 With approval, authorized employees may access, inspect or monitor the use of Information Resources without notice for investigative purposes, if there are reasonable grounds to believe a violation of College policy, agreements or applicable laws has occurred. Approval is required from a Vice President in accordance with Section 16.

Procedures

16.0 When there is reason to believe a violation of College policy, agreements or applicable laws has occurred, a Vice President may authorize the Director, Information Technology Services or other authorized personnel to access, inspect

and monitor Information Resources and, if necessary, take possession of a computer or portable storage device to determine if a user is acting in violation of Okanagan College policies, agreements or applicable laws.

17.0 A Vice President has the right to suspend an employee's or student's account or access to Okanagan College's networks, and the Director, Information Technology Services has the right to suspend a student's/other user's account or access to Okanagan College's networks, if there is an investigation into a possible violation of Okanagan College policies, Okanagan College agreements or applicable laws. This suspension may be made without prior notification.

18.0 Suspected violations by an employee are to be reported to the individual's supervisor and to the Director, Information Technology Services. Suspected violations by a student are to be reported to the Department Chair of the student's program and to the Director, Information Technology Services. Suspected violations by other individuals are to be reported to the Director, Information Technology Services.

19.0 The individual suspected of a violation will be informed of the suspension of privileges as soon as reasonably possible and may be invited to participate in the investigation. The employee's union will also be notified where applicable.

20.0 Investigations and penalties will be in accordance with Okanagan College policies where applicable and will depend on the nature and severity of the violation and the status of the user. If the violation is determined to be criminal in nature, the matter may be referred to appropriate law enforcement authorities.

21.0 The Vice President(s) will report to the President, as necessary, any inspections or monitoring of user accounts for violation of College policies.