8.1 Use of Information Technology

POLICY

College of the Rockies provides information technology resources to employees, students, and associates in order to further the teaching, learning, research, and administrative purposes of the institution. In certain situations, such as the Library, limited opportunities to use information technology resources may also be extended to members of the public.

SCOPE

All users of information technology provided by College of the Rockies must abide by this policy and any related rules and standards or risk loss of access to information technology and other penalties.

DEFINITIONS

Information Technology – Information technology encompasses all computing and communications facilities and services provided by College of the Rockies, including voice-mail and telephone service, computers, networks, accounts and storage, software, web pages and websites, and Internet access. It also encompasses services (for example, websites) hosted elsewhere when they are operated on behalf of the College.

GUIDELINES

A.

A.1 Privacy and confidentiality are important values for College of the Rockies. Normally, users can expect that their communications and the contents of their accounts will be treated as private and confidential and that their files will not be accessed without their permission. However, individuals have no right to absolute privacy when using information technology at the College. The College owns the information technology infrastructure and is responsible for its use. The College reserves the right to take action to see that its information technology is used lawfully, appropriately, and efficiently in pursuit of the primary purposes of the institution.

A.2 Privacy does not extend to the following situations:

A.2.1 Aggregate statistics about user accounts are not confidential (for example, data that indicates the amount of storage being used by particular accounts for .jpg files).

Authored by: Manager, IT Services Approved by: College Policy Committee Current issue date: May 2014
Scheduled revision date: May 2019

A.2.2 As a normal part of system administration, information technology employees monitor levels of network traffic, use software that logs network activity, make copies of files, and maintain archives of these copies.

A.2.3 Information technology employees may access any file, data, program, or e-mail in order to gather sufficient information to diagnose and correct network, hardware, and software problems. (See also the obligations of information technology employees in section 5.1, below.)

A.2.4 Information technology employees will compile and release otherwise confidential information when this is requested in accordance with section A.3 of this Policy.

A.3 The College information technology staff will gather and release information that is normally confidential only when specifically requested to do so and only when the request meets the following three conditions:

A.3.1 The request is made by the appropriate office in the institution. These offices are:

- The Executive Director of Human Resources with respect to compliance with Workers' Compensation legislation.

- The Coordinator, Information and Privacy (or another person authorized by the President to execute the legal obligations of the College with respect to legislation concerning freedom of information and protection of privacy) with respect to Freedom of Information requests or requests from law enforcement agencies for assistance with investigations.

- The Vice President-Education (in the case of students) or the Executive Director of Human Resources (in the case of employees and associates) with respect to an internal College investigation.

A.3.2 The request is made in writing, is reasonably specific in terms of the information required, and specifies to whom the information is to be released. The request to the Manager of IT Services to gather and release information need not contain reasons why the information is required. The person and office issuing the request according to section A.3.1 has the obligation to establish and document these reasons and to ensure that the request and subsequent actions comply with the appropriate laws and policies under which they are acting.

A.3.3 The request is addressed to the Manager of IT Services who shall be responsible for fulfilling the request, even though the actual work of gathering the requested information may involve other information technology employees.

A.4 The College does not guarantee the security of any messages or files sent or received through its networks. Although the College will employ various tools and methods to enhance network security, all users need to be aware that others can potentially intercept or accidentally receive data sent over a computer network.

A.5 The College assumes no liability for files and information that are stored on its systems. It has no obligation to maintain or destroy any or all physical representations of particular files.

B. OBLIGATIONS OF USERS

B.1 Legal Use

B.1.1 College of the Rockies requires all employees, students, and clients to use its information technology resources in ways that uphold all federal, provincial, and local laws and regulations. Areas of particular concern include:

- The Criminal Code of Canada. Threats, harassment, or others crimes committed electronically are crimes.
-
- Copyright Act. Storing, using, or displaying programs, images, music or data without the proper permissions is theft.
-
- Freedom of Information and Protection of Privacy Act. Information in an e-mail or on a website can easily be distributed beyond the intended audience and thereby infringe someone's right to privacy.

- Human Rights Code. All material that becomes public must respect the right of people to live in an atmosphere free of hatred, contempt, or discrimination. For example, it is illegal to display or print sexually explicit or racist material in a computer lab or in any other public context where others are likely to see it.

- Workers' Compensation legislation. The obligation to maintain a safe and healthy working environment is a broad one and includes specific requirements concerning workplace violence, threats, and discrimination.

B.2 Acceptance

B.2.1 In the use of information technology, as in many other activities, College students and employees are required to meet expectations and standards of professional and ethical behavior that go beyond the requirements of law.

These standards and expectation of "acceptable use" are designed to help achieve both (i) a positive learning and working environment in which all

persons treat each other with dignity and respect and (ii) the effective and efficient operation of information technology resources.

B.2.2 The requirements and expectations of acceptable use are contained in College of the Rockies policies, guidelines, and collective agreements and in the rules and standards that may from time to time be issued.

B.3 Using Information technology for non-College business

B.3.1 Occasional and incidental use of e-mail, voice mail, and Internet access for personal purposes is acceptable, provided that these uses, in the opinion of the College, do not:

- Interfere with institutional business (i.e., teaching, learning, research, and administration);
- Detract from an employee's availability to carry out his or her assigned responsibilities;
- Damage the College's reputation; and compromise the integrity and efficiency of the institution's information technology facilities and services.
- Compromise the integrity and efficiency of the institution's information technology facilities and services.

B.3.2 Use of College information technology and resources for commercial purposes or for the benefit of organizations not directly affiliated with College of the Rockies is forbidden without the written consent of the VP Finance. This includes, but is not limited to: any advertising on web pages or via e-mail or news postings; any solicitation of funds, goods, or services for any purpose; and processing or transmission of data on behalf of a third party whether a fee is charged or not.

B.3.3 All personal and approved commercial use of information technology resources has the same status as institutional use and is subject to the same expectations regarding legal and acceptable use.

B.4 Reporting possible illegal and unacceptable use

B.4.1 Employees should report to their supervisor all suspected illegal or unacceptable use of information technology resources.

B.4.2 Supervisors shall forward reports of possible illegal or unacceptable use to either the Vice President-Education (in the case students) or the Executive Director of Human Resources (in the case of employees). In the interests of efficiency, instructors can (in the case of students in their classes) report

cases of possible illegal or unacceptable use of information technology directly to the Vice-President Education, with a copy to the Dean of their Faculty.

C. OBLIGATIONS AND AUTHORITY OF INFORMATION TECHNOLOGY STAFF

C.1 Like all other members of the College community, employees who support the information technology infrastructure and provide information technology services are expected in the normal course of business to use information technology appropriately, respect the privacy of others, and maintain the confidentiality of information that may come to their attention during the routine exercise of their duties.

C.2 Information technology employees will ascertain and release information that is normally confidential only when specifically requested to do so according to the provisions of section A.3 of this Policy.

C.3 In situations where there is an immediate threat to the integrity and availability of the College's networks and data systems, technicians and administrators in information technology have the obligation and authority to take the measures that they, in their professional judgment, think are necessary to secure the networks and systems for general use, even if this means denying access and causing loss or inconvenience to some users.

D. SANCTIONS AND PROCEDURES IN CASES OF ALLEGED MISUSE

D.1 Investigating alleged misuse of information technology

D.1.1 College may undertake investigations of specific allegations of alleged misuse of information technology. These investigations may involve the collection and analysis of information that is otherwise considered private and confidential, subject to sections D.1.2 and A.3 of this Policy. The College will not engage in unannounced "fishing expeditions."

D.1.2 In the case of students, only the Vice President-Education may authorize investigations of alleged misuse of information technology. In the case of employees, only the Executive Director of Human Resources may authorize an investigation. In the case of the general public, only the Vice President-Finance may authorize an investigation. In cases where the identity of the person of interest is unknown, either the Vice President-Education or the Executive Director of Human Resources or the Vice President-Finance may authorize the investigation, but the further conduct of the investigation will fall to the appropriate person once the identity is known. All investigations must comply with the Policy provisions under which they are conducted—for example, notifying people that that their actions are under investigation and ensuring appropriate levels of confidentiality.

D.2 Processes for cases of alleged misuse

D.2.1 Within the College, the processes used to consider cases of alleged misuse of information technology will be those normally used for cases involving possible student or employee misconduct. Sanctions will include those allowed under various College policies, procedures, and collective agreements.

D.2.2 In addition to other sanctions, misuse of information technology may result in denial of access to the technology or specific limitations on its use. Any such denial or restriction must be reasonable in terms of time limits and extent.

D.2.3 The Vice President-Education, Vice President-Finance or the Executive Director of Human Resources has the authority to order the temporary withdrawal or limitation of privileges to use information technology pending a fuller investigation of alleged misuse.