KPU | KWANTLEN POLYTECHNIC UNIVERSITY

Policy History
Policy No. IM3
Approving Jurisdiction: President
Administrative Responsibility: Vice President Finance & Administration
Effective Date: June 4, 2011

Information and Educational Technology Usage Procedure

DEFINITIONS:

Data Encryption: Data encryption is a process of scrambling data to prevent anyone who does not have a decryption 'key' from using it.

IT Resources: Information and Technology resources refer to any information processing systems, services, infrastructure or the physical locations housing them. This includes computer labs, classroom technologies, computing and electronic communication devices, and services such as modems, email, networks and telephones.

Incidental Personal Use: Incidental Personal Use refers to use that is of a personal nature but that is brief and occasional; incidental personal use by students and staff is acceptable to the University as long as it does not interfere with the use of University resources for their intended purposes and, in the case of employees, as long as it does not interfere with their job performance.

Pornography: Pornography is the depiction of explicit sexual subject matter for the purpose of causing sexual excitement.

Pyramid Scheme: A pyramid scheme is a non-sustainable business model that involves the exchange of money primarily for enrolling other people into the scheme.

PROCEDURES

1. PRIVACY AND SECURITY

1.1 Users of the University's IT resources should have no expectation of privacy when using IT resources at the University. The University owns the information technology infrastructure and is responsible for its use. The University reserves the right to monitor usage and inspect data stored on its computer systems to ensure the high quality performance of systems or when the University believes that a violation of policy has occurred.

1.2 Information stored on the University's IT facilities are held in straight compliance with the University's policies C 4 Confidentiality of Students Records/Files, E 20 Freedom of Information and Protection of Privacy, and G 24 Confidentiality, except under the following situations:

1.2.1. Aggregate statistics about user accounts are not confidential (for example, data that indicate the amount of storage being used by particular accounts for certain kinds of files).

1.2.2. IT staff, as a normal part of system administration, monitor levels of network traffic, use software that logs network activity, make copies of files and maintain archives of these copies.

1.2.3. IT staff may access any file, data program or email in order to gather sufficient information to diagnose and correct network, hardware and software problems

1.2.4. IT staff will compile and release otherwise confidential information when this is requested in accordance with Section 1.3 of this Policy

1.3 The University IT 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:

1.3.1 The request is made by the appropriate office in the institution. It is the responsibility of the requesting office to ensure that the information is used in compliance with the Confidentiality Policy, G24, and protection of privacy legislation.

- Human Resources with respect to compliance with WorkSafeBC legislation
- The University Librarian (position responsible for managing the freedom of information and protection of privacy legislation) with respect to requests under the FOIPOP legislation or requests from law enforcement agencies for assistance with investigations

- The Associate Vice-President, Strategic Enrolment Management or the Registrar (in the case of students) or the Associate Vice-President Human Resource Services (in the case of employees) with respect to an internal University investigation

1.3.2 The request is made in writing, specifying the information required and to whom the information is to be released.

1.3.3 The request is made to the Executive Director, Information and Technology who shall be responsible for fulfilling the request.

1.4 Although the University will employ various tools and methods to enhance network security, the University does not guarantee the security of any messages or files sent or received through its networks.

1.5 The University assumes no liability for files and information that are stored on its systems and it has no obligation to maintain or destroy any or all physical representations of particular files.

2. INTELLECTUAL PROPERTY

2.1 Users must respect the legal protection provided by copyright laws for computer programs and data compilations and for all other works (literary, dramatic, artistic or musical). Also, users must respect the legal protection provided by trademark law and the common law for names, marks, logos and other representations that serve to distinguish the goods or services of one person from another.

2.2 Users must respect the rights of others by complying with all University policies regarding intellectual property regardless of medium.

3. FREEDOM OF EXPRESSION

3.2. While the University will make every effort to screen incoming data for viruses, worms, etc., it is not the practice of the University to screen or control the information that is otherwise available on its network. However, the University will comply with any court orders or legislation that bans specific information.

3.3. Users are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media. Contents published through the University's IT facilities are subjected to this policy and related procedures.

3.4. When publishing content to any website outside of the University, users must make it clear that the postings do not represent Kwantlen's position, strategies or opinions. Do not provide confidential information of Kwantlen's or another organization or individuals.

4. APPROPRIATE AND RESPONSIBLE USE

The following provides an outline of the appropriate and responsible use of the University's IT resources:

4.1 Respect the legal protection provided by copyright and license to programs and data as outlined in section 2.1 above

4.2 Respect the rights of others by complying with all University policies and Collective Agreement provisions regarding sexual, racial and other forms of harassment and by preserving the privacy of personal data to which you have access.

4.3 Respect the privacy of others by not tampering with their files, discs, passwords or accounts or representing others when messaging or conferencing.

4.4 Use only computer Identification codes or accounts and communication facilities which you are authorized to use and use them for the purposes for which they are intended.

4.5 Respect the integrity of computing systems and data; for example, by not intentionally developing programs or making use of already 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

5. ILLEGAL AND UNACCEPTABLE USES

The following, while not exhaustive, provides examples of illegal and unacceptable uses of the University's electronic resources:

ILLEGAL USES

5.1 Uttering threats by any electronic means

5.2 Distributing pornography to minors

5.3 Child pornography

5.4 Pyramid schemes

5.5 Gambling or betting

5.6 Making unauthorized copies of proprietary software or offering unauthorized copies of proprietary software to others

5.7 Infringement of copyright, trademark or other intellectual property rights

UNACCEPTABLE USES

5.8 Seeking information on passwords or data belonging to another user

5.9 Copying someone else's files or programs or examining such information unless authorized

5.10 Attempting to circumvent computer security methods or operating systems
5.11 Downloading of files that could potentially damage the University's information and technology systems
5.12 Using University-provided computer accounts for commercial purposes such as promoting profit-driven products or services
5.13 Intercepting or examining the content of messages, files or communications in transit on a voice or data network
5.14 Interfering with the work of other users of a network or with their host systems (e.g. chain letters or spamming) or engaging in any uses that result in the loss of another user's files or systems
5.15 Harassing, defamatory, derogatory, discriminatory or false voice or data messages
5.16 Sending, receiving or accessing offensive, objectionable, abusive, pornographic, obscene, sexist, racist, harassing or provocative messages, images or other materials including adult-oriented web sites or news groups. This does not apply to the use of such material in the course of conducting scholarly research.
5.17 Political activities
5.18 Unauthorized solicitation of funds
5.19 Unauthorized disclosure of confidential or privileged information
5.20 Unauthorized use of data encryption

6. RIGHTS OF AUTHORIZED EMPLOYEES

6.1 Authorized employees have the right to take whatever appropriate measures are required to ensure the integrity and availability of the University's IT resources.
6.2 Material stored on the University's information systems and networks will be removed in a timely manner if it is found to be in violation of section 5 of these procedures, "Illegal and Unacceptable Uses".
6.3 As part of the normal activity of system administration, authorized employees have the right to examine files, data and mail in order to gather sufficient information to diagnose and correct system hardware and software problems or to determine if a user is acting in violation of the policies stated in this document.
6.4 Authorized employees must have sufficient reason to conduct the kind of investigation outlined in 6.3 and must obtain the permission of the Executive Director, Information and Technology in order to carry out the investigation.
6.5 Employees carrying out such an investigation have an obligation to maintain the privacy of a user's files, data and mail.

7. REPORTING AND INVESTIGATION

7.1 Every Kwantlen Polytechnic University employee has an obligation to report any information that is important to the safety and security of the University and/or its students and employees.

7.2 Violations of any portion of this Policy and related Procedures will be dealt with in accordance with the Code of Conduct Policy and Procedures, C21.

7.3 If the violation constitutes a breach of federal, provincial, local laws or statutes, law enforcement agencies will also be notified.

8. RULES AND STANDARDS

8.1 In order to promote a positive working and learning environment and to ensure that the University's limited electronic resources are used effectively and efficiently, the Department of Information and Technology envisages the need to develop various rules and standards on a wide variety of topics related to information technology, for example: standards for equipment connecting to the network, quotas on network storage and expectations of email etiquette.

8.2 These rules and standards will be developed as Departmental Practices and will be issued with the approval of the Executive Director, Information and Technology and the Vice-President, Finance and Administration.

RELATED POLICY

Refer to IM3 *Information and Educational Technology Usage Policy*