KWANTLEN POLYTECHNIC UNIVERSITY

Policy History
Policy No. IM3
Approving Jurisdiction: President
Administrative Responsibility: Vice President Administration
Effective Date: July 13, 2022

Information Technology Usage Procedure

A. DEFINITIONS

1. **Data Encryption:** Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission.

2. **Incidental Personal Use:** Incidental Personal Use refers to use that is of a personal nature that is unrelated to the University or to one's professional development, studies or employment at the University 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, is consistent with the University's policies and, in the case of employees, as long as it does not interfere with their job performance.

3. **KPU Technology Resources:** KPU technology resources include but are not limited to computer networks, systems, servers, software, (including subscriptions, licenses), databases, shared and collaboration digital platforms, University social media platforms, digital storage, equipment and devices, email, wireless cloud services and the University internet connections.

B. PROCEDURES

1. AUDITS
    a. KPU performs periodic reviews to ensure policy compliance.

2. ENFORCEMENT

   a. This Policy will be enforced by KPU's Chief Information Officer. Breaches of this Policy and its related Procedure may be subject to the full range of disciplinary actions available to the University and may result in the denial of access to KPU Technology Resources.

3. ACCEPTABLE USE

   a. Authorized users are permitted to use KPU's Technology Resources and services for the purpose of:

      i. Administrative functions
      ii. Teaching and Learning
      iii. Research
      iv. Limited Incidental Personal Use

4. PASSWORDS

   a. Passwords must comply with the Information Security Standard Passphrase and Password Protection to ensure that only authorized individuals are permitted access to KPU's computer systems and data.

      i. Passphrase/Passwords secure computers against potential assaults from the cybercriminals who break into systems and steal identities to commit crimes.

      ii. Passwords must conform to the following:

         1) Be kept confidential.
         2) Never be shared with anyone, or used in plain sight of others.
         3) Be committed to memory and never written down
         4) Be changed annually or as directed by password policy guidelines.
         5) Passwords used for personal or non-KPU accounts (i.e. Social Media, Banking, etc.) must not be used for KPU systems).

5. PRIVACY AND ACCESS TO INFORMATION

The University is subject to the Freedom of Information and Protection of Privacy Act of BC ("FIPPA" or "the Act") which sets out the University's privacy obligations and access to information requirements. Users of the University's Technology Resources must be aware that:

   a. Personal information stored in University Technology Resources for KPU business purposes will be protected under the Act;
   b. Incidental personal use of KPU Technology Resources is permitted in accordance with section 6 Personal Usage, however KPU is not responsible for privacy protection of personal information not required for KPU business purposes;
   c. All records in the custody or control of the University are subject to access to information requests and any record created or held by a KPU Employee may be required to fulfill the University's requirements under the Act;
   d. Users are encouraged to limit the personal information they include in their personal use of KPU Technology Resources.

6. PERSONAL USAGE

    a. Incidental Personal Use of KPU's Technology Resources is permitted but must not have a negative impact on KPU Technology Resources, the University community, or on any user's job performance. KPU reserves the right to audit and monitor the usage of KPU's Technology Resources and its content at any time without prior notice.

    b. KPU is not responsible for managing, backing up, recovering lost or supporting any personal information such as, but not limited to personal files, emails, data, applications, photos, videos, or music stored on KPU's Technology Resources. KPU reserves the right to remove or delete any information stored on KPU Technology Resources without prior notice.

7. PERSONAL RESPONSIBILITY

    a. KPU requires users to use Technology Resources responsibly and in accordance with KPU's policies. Inappropriate use of KPU Technology Resources may result in loss or damage to the university or others. If KPU suffers loss or damage related to inappropriate use of KPU's Technology Resources, KPU may seek to hold the individual user liable and recover repair or replacement costs. KPU will also seek to recover any or all usage cost associated to personal use of KPU's Technology Resources (i.e. personal data or voice charges on a KPU issued smartphone devices).

        i. In using KPU's Technology Resources for anything but KPU's business in accordance with KPU policies, users are accepting the risk of such liability. Employees and must return all KPU Technology Assets assigned to them upon termination of employment. Student loaned devices must be returned as agreed to with the university.

        ii. The University expects that employees and students will take reasonable measures to ensure the physical security of KPU Technology Assets. Employees and students could be held liable for inappropriate use or mishandling of KPU's Technology Assets resulting in loss, theft, or damage. KPU may seek compensation equal to repair or replacement cost in such cases.

8. UNACCEPTABLE USE EXAMPLES

    a. The following actions constitute unacceptable use of KPU's Technology Resources. This list is not exhaustive but is included to provide a frame of reference for types of activities deemed unacceptable. The authorized user must not use any of KPU's Technology Resources to or for:

        i. Unauthorized access to KPU Technology Resources including systems and data.

        ii. Use of software, cloud services and digital subscriptions on KPU Technology Resources without IT, Teaching and Learning Commons and/or Office of Research Services approval. For a list of authorized software, cloud services and digital subscriptions contact the IT Service Desk.

        iii. Use of personal or unauthorized computing devices to access KPU Technology Resources beyond KPU guest wireless access.

        iv. Reveal system or network credentials (IDs or passwords) to others

        v. Engage in copyright infringement, install or distribute unlicensed or "pirated" software.

vi. Engage in any activity that negatively impacts the performance of KPU Technology Resources.

vii. Engage in activity that impedes the operations or delivery of University services.

viii. Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, introduction of viruses/malware or other IT information gathering techniques when not part of the user's job function.

ix. Engage in phishing or spamming activities.

x. Engage in activities that cause disruption to the workplace environment or create a hostile workplace.

xi. Disseminating defamatory, discriminatory, or harassing content (unless an exception is approved in writing by the President or Provost for academic or research purposes).

xii. Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the university and its community.

xiii. Engage in activity that gives rise to a criminal offense or otherwise violates federal or provincial statutes.

xiv. Engage in activity that may reasonably result in civil law suits.

xv. Engage in activities that are non-compliant with applicable privacy laws.

xvi. Engage in activities that are of a personal business or for-profit nature.

xvii. Disseminate solicitation communications that make fraudulent offers for products and services.

C. RELATED POLICY

AD2 *Student Complaints about Instruction, Services and Employees*
AR3 *Confidentiality of Students Records/Files*
IM1 *Copyright Compliance*
IM3 *Information Technology Policy*
IM2 *Freedom of Information and Protection of Privacy*
IM4 *Confidentiality Policy / Procedures*
IM9 *Information Security*
ST2 *Student Academic Integrity*
ST7 *Student Conduct (Non-Academic)*