|  |  |
| --- | --- |
| ubclogo.jpg | Faculty of Medicine, Dean’s Office  Policies, Procedures, & Guidelines Information Technology Usage Agreement |

# Appropriate Use

The computing and communications facilities and services provided at the University of British Columbia are primarily intended for teaching, research, and administrative purposes. Their use is governed by all applicable University policies, as well as all applicable Canadian federal, provincial and local laws and statutes. This document adds to existing University policies and as such it is the individual’s responsibility to read and adhere to all applicable UBC policies in addition to this document.

**Responsible use of computing facilities and services includes:**

1. Respecting the legal protection provided by copyright and license to programs and data.
2. Respecting the rights of others by complying with all University policies regarding intellectual property.
3. Respecting the rights of others by complying with all University policies regarding sexual, racial and other forms of harassment, and by preserving the privacy of personal data to which you have access.
4. Respecting the privacy of others by not tampering with their passwords or accounts, or representing others when messaging or conferencing.
5. Respecting the privacy of others by not sharing material or information that you are exposed to in the course of carrying out your duties.
6. Using only computer IDs or accounts and communication facilities which you are duly authorized to use and using them only for the purposes for which they were intended.
7. Respecting the integrity of computing systems and data; for example, do not intentionally develop programs or make use of already existing programs that harass other users or infiltrate a computer or computing system, or gain unauthorized access to other facilities accessible via the network.
8. Using computing and communications facilities in a manner which is accountable and consistent with the ethical principles set forth by the University and with accepted community standards.
9. Respecting and adhering to any local, provincial or federal law which may govern use of these computing and communication facilities in Canada, including the Criminal Code of Canada, the BC Civil Rights Protection Act, the BC Freedom of Information and Protection of Privacy Act, and the BC Human Rights Act.Computer Guidelines
10. To maintain security, IDs and passwords are not to be shared by individuals. If necessary, please contact your supervisor, who will work with MedIT to assign user IDs with appropriate rights.
11. To maintain accountability all users and computers must be logged onto the domain for network authentication and access to resources.
12. Passwords need to be changed regularly and consist of non-dictionary words at least eight characters in length and contain a minimum of 3 out of 4 of the following character types. English uppercase characters (A through Z).

* English lowercase characters (a through z).
* Base 10 numbers (0 through 9).
* Non-alphabetic characters (for example, !, $, #, %).

Passwords cannot be changed more than once a day and they must not be reused; the system remembers the last four passwords that an individual used.

For examples on how to set up passwords that are secure and easy to remember, please see MedIT’s best practices at <http://medit.med.ubc.ca/Resources/password.htm>

1. Dean’s Office computers, computer IDs, accounts, and other communications facilities are to be used for authorized purposes. Incidental personal use is acceptable as long as it does not interfere with use of the facility for its intended purpose and, in the case of employees, as long as it does not interfere with his or her job performance or the performance of other employees.

* Dean’s Office computers are not to be used to store personal or non-work related files (music, videos and photos) on either the C-Drive or the U-Drive.

1. The Faculty of Medicine, Dean’s Office accepts that there may be incidental use of social networking or other personal use websites. Use of social networking or personal use websites is not acceptable in cases where this use negatively impacts on one or more employees’ productivity or their contribution to office work.
2. For security purposes, files need to be handled as follows:

* Do not save anything locally on the computer. Files should be kept in designated areas on network drive shares to ensure that they are stored securely and backed up every night. Please contact your supervisor to determine the appropriate location to store shared files.
* Information stored on portable storage devices (USB Flash Drives, Laptops, Smart Phones (Blackberry, iPhone, Windows Mobile, Android, etc), Personal Digital Assistants (PDAs), external hard drives, etc.) that is classified as personal information, or information that could be considered damaging to the Faculty of Medicine or the University must be fully encrypted. Contact MedIT for assistance with securing this data.

1. Viruses: Should the antivirus software detect a virus, please report the incident immediately to the MedIT Help Desk, together with the probable source of infection. If necessary, request assistance to ensure the software has repaired or removed the virus before accessing the file.
2. Email:

* Refer to MedIT’s E-mail Best Practices at <http://medit.med.ubc.ca/faq/MedIT_E-mail_Best_Practices.htm> and UBC IT’s information on Exchange <http://www.it.ubc.ca/email/exchange/usingexchange.html>
* Dean’s Office email is not to be used for the disclosure of confidential information, pornography, profanity, transmission of viruses or worms, material protected by copyright and SPAM.
* If a document is considered too confidential to fax, it should not be emailed.
* Do not open suspicious emails. If your antivirus software detects a virus, do not open the file. Report the incident immediately to the MedIT Help Desk.
* Email storage: User accounts have storage limits on the mail server. Too many messages, especially those with large file attachments can consume considerable space. If you wish to retain a message, store it in a Personal Folder rather than in a folder in your email Inbox.
* Dean’s Office Internal Communications maintains all email groups for the Dean’s Office in order to adhere to best practices on the management of those groups.
* The use of email for personal messages is a privilege and it is important to understand that there are limitations.
* Personal email must be stored in a separate file which can be copied to disk and deleted should the employee leave the Dean’s Office.
* Always be aware that email is not guaranteed to be private.

1. Telecommuting:

* Employees require prior written approval from your supervisor.
* Employees must adhere to appropriate Telecommuting guidelines and/or policies.

1. Do not download or install software on your computer. Only MedIT is authorized to make installation, setup or configuration changes to computer software or hardware on PCs, loaner laptops, and the network.
2. If you encounter computer problems: note the date and time of the problem, the software application you were using at the time, the document you were working on when the problem occurred (if applicable) and any error message(s) you receive on your screen at the time. Contact the MedIT Help Desk and provide them with that information so that they may assist you.
3. The Dean’s Office loaner laptops may be used by Dean’s Office employees only, must be used only for Dean’s Office business, and must be signed in and out via the Order Desk on the 3rd floor of IRC.
4. To maintain your computer:

* Dust your keyboard, mouse, computer and monitor regularly.
* Ensure adequate computer ventilation.
* Use a static mat under your chair to prevent static electrical short circuits.
* Keep food and drink away from keyboards and terminals.
* Use one of the standard screen savers provided with your system.
* Use a surge-protector to protect against random power fluctuations.

1. For security and safety reasons, when your computer will be left unattended, lock your computer by pressing the Windows Logo Key + “L”. At the end of each day turn off your monitor, but do not turn off your computer.

The user bears the primary responsibility for the material that he or she chooses to access, and or display on his or her computer. The computer facilities may not be used in any manner which contravenes the above policies, laws or statutes. Those who do not adhere to these guidelines may be subject to suspension of computing privileges.

**Telephone Guidelines**

1. Each month telephone, Blackberry, cellular and pager charges will be reviewed by Accounts Payable and the Purchasing Coordinator. Excessive charges will be brought to the attention of the subscriber.
2. Rogers, Bell and TELUS bills will be distributed to the reconcilers of the PGs they are charged to. The PG reconciler is responsible for reviewing the charges with the subscriber and the subscriber is responsible for submitting the amount for personal calls.
3. If you encounter problems with Blackberry devices, contact the MedIT Help Desk at 2-7649.
4. Only MedIT is authorized to make installation, setup or configuration changes for Blackberry devices.

All communication equipment, including telephones, should be used for authorized purposes only with minor incidental personal usage being acceptable as long as it does not interfere with job performance or result in unreasonable additional charges to the Faculty.

This policy shall not be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties.

Signature of Dean’s Office member denotes that the individual takes responsibility for reading, understanding and accepting the appropriate use and guidelines as outlined above.

I agree to abide by the above conditions:

Name:

Signature:

Date: