Title:	**RESPONSIBLE USE GUIDELINES**
Reviewed:	June 28, 2013
Audience:	Faculty, administrative staff, students and users of the Faculty of Medicine network
Purpose:	To outline the acceptable use of computer equipment at the Faculty of Medicine
Contact:	MedIT

1 Overview

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. See also, specific policies related to UBC network services.

The user bears the primary responsibility for the material that he or she chooses to access, and or display. 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.

2 Purpose

The purpose of these guidelines is to outline the acceptable use of computer equipment at the Faculty of Medicine. These rules are in place to protect the user and the Faculty of Medicine. Inappropriate use exposes the Faculty of Medicine to risks including virus attacks, compromise of network systems and services, and legal issues.

3 Scope

These guidelines apply to Faculty, administrative staff, students and users of the Faculty of Medicine network. These guidelines apply to all equipment owned or leased by the Faculty as well as any equipment attached to the FoM network.

4 Guidelines

4.1 Responsible Use of Computing Facilities and Services

- Respect the legal protection provided by copyright and license to programs and data
- Respect the rights of others by complying with all University policies regarding intellectual property
- Respect 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
- Respect the privacy of others by not tampering with their tapes, passwords or accounts, or representing others when messaging or conferencing

- Use only computer IDs or accounts and communication facilities that you are duly authorized to use, and use them for the purposes for which they were intended
- 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 gain unauthorized access to facilities accessible via the network
- Use computing and communications facilities in a manner that is consistent with the ethical principles set forth by the University and with accepted community standards.
- For security and network maintenance purposes, authorized individuals within the Faculty of Medicine may monitor equipment, systems and network traffic at any time, per the FoM Audit Policy
- Respect and adhere to any local, provincial or federal law which may govern the 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

4.2 Email and Communications Activities

- Refer to UBC IT Guidelines
- Faculty of Medicine email is not to be used for the disclosure of confidential information, pornography, profanity, transmission of viruses or worms, material protected by copyright, transmission of messages through an open SMTP relay, or spam
- Faculty of Medicine equipment and services are not to be used for any form of harassment via email, telephone or paging, whether through language, frequency or size of messages
- Users must not misrepresent their identity as senders of messages or the content of such messages
- Employees must understand the privilege and limitations of personal email use

5 Compliance

Any user found to have violated this policy may be subject to a range of disciplinary action from loss of access privileges to prosecution under Criminal Law.

Any user found to have violated this policy may be subject to a range of disciplinary action from loss of access privileges to prosecution under Criminal Law.

6 Definitions

Spam – Unauthorized and/or unsolicited electronic mass mailings.

Any user found to have violated this policy may be subject to a range of disciplinary action from loss of access privileges to prosecution under Criminal Law.