



## **AIDS COMMUNITY CARE MONTREAL • SIDA BÉNÉVOLES MONTRÉAL**

### **COMPUTER AND INTERNET USE POLICY**

#### **1. PURPOSE**

The purpose of this policy is to provide employees and volunteers with general requirements for utilizing the organization's computers, networks and Internet services.

These are general guidelines and examples of prohibited uses for illustrative purposes, but do not attempt to state all required or prohibited activities by users. Employees and volunteers who have questions regarding whether a particular activity or use is acceptable should be addressed to the System Administrator or Executive Director. The System Administrator is designated by Executive Director.

Compliance with this policy is obligatory.

#### **2. ACCESS TO COMPUTERS, NETWORKS AND INTERNET SERVICES**

The level of access that employees and volunteers have to computers, networks and Internet services is based upon specific employee or volunteer job requirements and needs.

#### **3. ACCEPTABLE USE**

- a) Employee and volunteer access to the organization's computers, networks and Internet services are provided for administrative, educational, communication and research purposes, consistent with the organization's mission. General rules and expectations for professional behaviour and communication apply to use of the organization's computers, networks and Internet services.
- b) Employees and volunteers are to utilize the organization's computers, networks and Internet services for work-related purposes and performance of job duties. Incidental personal use of organization computers is permitted outside of work hours as long as such use does not interfere with the employee's job duties and performance, with system operations or with other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications.

#### 4. PROHIBITED USE

- a) The employee or volunteer is responsible for his/her actions and activities involving ACCM's computers, networks and Internet services, and for his/her computer files, passwords and accounts. General examples of unacceptable uses, which are expressly prohibited, include, but are not limited to, the following:
- i) Any use that is illegal or in violation of other ACCM policies, including harassing, discriminatory or threatening communications and behaviour; violations of copyright laws, etc.;
  - ii) Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive unless for work purposes;
  - iii) Any inappropriate communications with other parties;
  - iv) Any use for personal financial gain, or commercial, advertising or solicitation purposes;
  - v) Downloading or loading software or applications without permission from the System Administrator or Executive Director;
  - vi) Opening or forwarding any e-mail attachments (executable files) from unknown sources/that may contain viruses;
  - vii) Sending mass e-mails to organization users or outside parties for organization or non-organization purposes without the permission of the Executive Director or director of the department concerned;
  - viii) Any malicious use or disruption of the organization's computers, networks and Internet services or breach of security features;
  - ix) Any misuse or damage to the organization's computer equipment;
  - x) Misuse of the computer passwords or accounts (employee or other users);
  - xi) Any communications that are in violation of generally accepted rules of network etiquette/professional conduct;
  - xii) Failing to report a known breach of computer security to the System Administrator or Executive Director;
  - xiii) Any attempt to delete, erase or otherwise conceal any information stored on an organization computer that violates these rules.
  - xiv) Changing software parameters on a computer without permission from the System Administrator or Executive Director. (ie: turning off automatic updates or system restore; this does not apply to user preferences)

#### 5. NO EXPECTATION OF PRIVACY

The organization retains control, custody and supervision of all computers, networks and Internet services owned or leased by the organization. The organization reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of organization computers, including e-mail messages and stored files.

## 6. CONFIDENTIALITY OF INFORMATION

Employees are expected to observe all aspects of *ACCM's Confidentiality Policy* in their use of computers, networking and the internet.

## 7. SUPERVISORY RESPONSIBILITIES OF EMPLOYEES AND VOLUNTEERS

Employees and volunteers are expected to be familiar with the organization's policies and rules concerning computer and Internet use and to enforce them. When, in the course of their duties, employees, Employees or volunteers become aware of violations, they are expected to stop the activity and inform the System Administrator or Executive Director.

## 8. ORGANIZATION ASSUMES NO RESPONSIBILITY FOR UNAUTHORIZED CHARGES, COSTS, OR ILLEGAL USE

The organization assumes no responsibility for any unauthorized charges made by computer users, including but not limited to credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

## 9. DATABASE MANAGEMENT

Each department is responsible for the maintenance and security of its respective database(s). Database(s) are not to be included as part of a shared network and must be protected by a password. Database(s) must be backed up monthly.

## 10. BACK UP FILES

Each department is responsible for the maintenance and back up of their respective files. Regular, monthly back ups of files are necessary to ensure continuity within the organization. Semi-annually each department will be requested a back up of its database(s) on a "mini-CD" to be stored in the safety deposit box at the bank.

## 11. DISCLAIMER

Each email sent on behalf of the organization needs to include the default disclaimer text. Each email account is set up with this text and can not to be modified unless permission is given by the Executive Director.

— *Adopted 25 October 2005*