

THE ALMA MATER SOCIETY OF THE UNIVERSITY OF BRITISH COLUMBIA

AMS Student Society
 6138 SUB Boulevard
 Vancouver, BC V6T 1Z1
www.ams.ubc.ca



Number & Title #I-6 - *Responsible Computer Use*

Effective Date:

April 9, 2015

Approval Date:

April 9, 2015

Policy Type

Internal Policy

Review Date:

This policy shall be reviewed every two (2) years.

Responsible Body:

Student Life and Communications Committee

Authority:

AMS Code of Procedure Section II, article 11(1)

“Council may create external and internal policies as well as combined policies.”

Purpose and Goals:

This policy is designed to:

- 1) Outline best practices around the use of AMS computers and computing systems;
- 2) Protect the *Society's* computers and computing systems from damage.

Applicability:

This policy is applicable for all employees, appointees, and elected officials of the AMS.

Exclusions:

There are no exclusions for this policy.

Definitions:

For the purposes of this policy and in all other policies in which they are not otherwise defined:

Users shall mean employees, appointees, elected officials, and all others who use *AMS* computers and/or computing systems.

AMS IT shall refer to the department within the *AMS* responsible for Information Technology.

Policy:

GENERAL

- 1) All *Society Users* shall, in their use of the *Society's* computers and computing systems, conduct themselves in accordance with established business ethics and in accordance with the responsibilities of their respective positions.
- 2) The *Society's* computers and computing systems are the property of the *Society*, and are for utilization by *Users* for business purposes only. The use of computing resources for any purposes not pertaining to their position will be considered unauthorized.
- 3) *AMS IT* shall have the power to redistribute computing resources as necessary in order to ensure the efficient use of *Society* resources.
- 4) The *Society* shall not monitor the email or files of *Users* without their knowledge, except when the *Society* or its systems may be harmed. Situations when the *Society* may monitor computer use include, but are not limited to, suspected criminal activity, excessive attachment use, and virus infection.
- 5) The acquisition of any computer hardware must be processed through *AMS IT* to ensure compatibility with the *Society's* systems and be approved by the *AMS VP Finance* for the governance branch of the *Society* or the relevant *Business Head* for the business branch of the *Society*.

- 6) Any damage to computers or computing systems caused by inappropriate or unauthorized personal use by a *User*, and any other violations of the provisions of this Policy, may result in disciplinary action by the *Society*.

ELECTRONIC COMMUNICATION

- 7) When using the *Society's* email, *Users* shall not:
 - a. Log in to an email account that they are not authorized to access;
 - b. Impersonate another user by any means including but not limited to falsifying header or user identification information;
 - c. Create or distribute any disruptive or offensive material, including illegal, abusive, indecent, defamatory, obscene or menacing materials;
 - d. Operate in breach of confidence, copyright, or privacy rights;
 - e. Initiate or forward spam, including chain letters, pyramid schemes, hoaxes, joke emails, or unsolicited mail;
 - f. Send virus warning emails without approval by the AMS IT Manager.
- 8) Any incoming or outgoing email message which is suspected of containing a virus or malicious attachment, or which could be detrimental to the *Society's* network, may be isolated for inspection. The message will be released by *AMS IT* to the intended recipient only after it is determined to be risk free.

COMPUTER USE

- 9) All *Users* shall make every effort to support the *Society's* Information Technology (IT) Department in protecting the security of the *Society's* technical systems. As such, *Users* shall not:
 - a. Knowingly install, download, or forward a virus for any purpose;
 - b. Share password or login information;
 - c. Access computers or accounts which they are not authorized to access;
 - d. Remotely access *Society* servers and workstations on infected or otherwise compromised devices.

- 10) All software installed on the *Society's* computing resources must be approved by *AMS IT*.
- 11) Remote access to the *Society's* IT resources and the installation of computing devices not owned by the *Society* on the *Society's* network requires the permission of *AMS IT*.
- 12) It is prohibited to use the *Society's* computer system and internet connection to:
 - a. Access websites containing sexually explicit, racist, violent, or generally offensive materials, except to carry out research for the *Society*;
 - b. Distribute to internal or external users material containing sexually explicit, racist, violent, or generally offensive material;
 - c. Download and/or illegally use unlicensed software;
 - d. Act in violation of the Criminal Code or the BC Human Rights Code;

Consultations

The following groups have been consulted during the development of this policy:

Director of Finance and Administration, AMS IT Manager, Legislative Procedures Committee. Student Life and Communications Committee.

History:

This is the third draft of the second version of this policy.

Related Policies:

There are no policies related to this policy.

Appendix:

There is no appendix to this policy.