Information Technology Acceptable Use Procedures

Prepared By: David Arbuthnot
VP, IT

Date Prepared: June, 2001

Revised By: Paul Athaide
Manager, Infrastructure Services

Date Revised: January 24, 2017

Version 2.4

Contents

1.0 Policy Procedures

This policy defines the appropriate use of computing and communications resources. This policy addresses the information stored on or transferred via computers, networks, telephones, mobile devices or other communications devices, as well as the usage and protection of the physical assets themselves. This policy applies to all employees and volunteers with access to Society computing and communication resources.

2.0 Policy Statement

The intent of this Acceptable Computer Use Policy is not to impose restrictions that are contrary to the MS Society's established culture of openness, trust and integrity. Rather, this Policy is published to protect the MS Society's staff, volunteers and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

The MS Society's computer network has been designed, purchased, and installed primarily for one purpose: to facilitate communication between MS Society personnel and volunteers internally and between the MS Society and third parties having an interest in our organization. The computers and all of the information in the network are the property of the MS Society in exactly the same sense as other MS Society equipment and paper records. Users are required to consistently follow established operating and security procedures in order to protect the MS Society's business and its operations with vendors and clients. This policy is in effect at all times and not just during regular working hours

It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

3.0 Acceptable Usage

3.1 General

No expectation of privacy.

The computers and computer accounts given to users are to assist them in performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send or receive on any computer resource. The computer resources belong to the MS Society of Canada and may be used only for business purposes.

Waiver of privacy rights.

Users expressly waive any right of privacy in anything they create, store, send, or receive through use of the computer resources or through the Internet or any other computer network. Users consent to allow personnel of the MS Society of Canada, authorized by the National President & Chief Executive to access and review all materials users create, store, send, or receive on the computer or through the Internet or any other computer network. Users understand that the MS Society of Canada may use human or automated means to monitor use of its Computer Resources.

Monitoring of computer usage.

The MS Society of Canada has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users to the Internet, reviewing e-mail sent or received by users and monitoring the amount of time users spend in any of the above activities.

Inappropriate or unlawful material

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication (such as bulletin board systems, news groups, chat groups) or displayed on or stored in the MS Society of Canada's computers. Failure to comply will be handled through the MS Society of Canada's National Workplace Relationship Policy. Users encountering or receiving this kind of material should remove it immediately, advise the source to cease transmissions of this nature and report the incident to their supervisors.

Disclaimer of liability for use of Internet

The MS Society of Canada is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.

Intellectual Property

All creation of intellectual work, such as software development, promotional material or presentations, using the MS Society of Canada equipment, including PC's, are the property of the MS Society of Canada. Any reproduction, distribution or modification of data or programs requires authorization from the MS Society of Canada. The MS Society of Canada employees are responsible for honoring the intellectual property rights of the MS Society of Canada and of fellow employees.

3.2 User Responsibilities

MS Society computer users have an obligation to use their access to Internet and other electronic networks in a responsible and informed way, conforming to the policy and communicating professionally.

General user obligations are:

- Do not engage in any activity that is illegal under local, provincial, federal or international law while utilizing MS Society resources and systems.
- Respect statutory provisions against the unauthorized disclosure or collection of personal, Third party and other sensitive information
- Notify the *Privacy Officer* when there has been an unauthorized disclosure of sensitive information.
- Be accountable and responsible for the content of transmitted messages and attachments as well as ensuring that sensitive information is not disclosed.
- Take all reasonable precautions to protect your account, including password maintenance and file and directory protection measures.
- Be aware of computer security issues and guard against computer viruses.

3.3 Unlawful and unacceptable conduct

Any activity using MS Society electronic networks that is that is illegal under local, provincial, federal or international law is not permitted. Some examples include:

- Knowingly causing congestion on computing resources or interfering with the work of others
- Using on computing resources for commercial or financial gain
- Using, sending or accepting copyrighted materials without permission (i.e. Music or Videos)
- Creating, copying or transmitting chain letters or other non-MS Society related mass mailings, regardless of the subject matter
- Vandalizing on computing resources, including the uploading or creation of computer viruses
- Falsifying one's identity while using computing resources
- Installing unauthorized software on computing resources
- Circumventing security and/or authentication measures. This includes, but is not limited to, attempts to discover another user's password, taking resources from other users, distribution or execution of a program that damages another user's files or MS Society computing resources and gaining access to resources, programs, or data for which proper authorization has not been given.
- Physically tampering with MS Society's computing resources
- Deliberately attempting to degrade system performance or deprive authorized users access to MS Society computing resources (i.e.: running of programs or processes which will slow network or system response to the point of restricting others access)
- Destroying or altering corporate records without authorization
- Disclosing or collecting sensitive information without authorization
- Copying, renaming, changing, examining, or deleting files belonging to someone else without authorization.

3.4 Use of Internet

- *Access* - While Internet access is primarily for business purposes, Users are permitted to access the Internet for personal use, in strict compliance with the other terms of this Policy.
- *Confidentiality Issues* - There is no guarantee of privacy or confidentially of information on the Internet. Users are advised that no privacy rights exist in personal or business information transmitted and are specifically directed not to transmit production, financial, sales/marketing, trade secrets, or other confidential information that might affect the MS Society's competitive position, serve to embarrass the MS Society or its employees, or compromise privacy laws. Users are specifically prohibited from using Internet access to penetrate private networks of other Companies for any purpose, unless under an existing agreement with the Company owning the network.
- *Legal Issues*- Unless specifically otherwise noted, all information on the Internet, including software, should be considered as copyrighted material. Users are prohibited from downloading such materials, including software, and/or modifying such files without the permission of the copyright holder. Where such downloading occurs, the MS Society, as well as the User, may be subjected to civil and criminal penalties under the applicable federal and provincial copyright laws. All questions with regard to the legality of downloading materials from the Internet must be referred to the I.T Department or General Counsel for review and approval, prior to downloading.
- *Auditing*- The MS Society has a right and may audit a User's Internet transactions both to and from the Internet without notice to any User that such audit is about to begin or has been performed. If violations of the MS Society's Acceptable Use Guidelines are found, disciplinary action will be assessed, including, if appropriate, termination (other corrective actions for non-employees) depending upon the seriousness of the violation.

3.5 E-Mail

E-mail should be used primarily for business purposes only. From time to time, users may use e-mail for personal purposes provided it is: i) on their own time and ii) in no way adversely affects their job performance. Use of e-mail to send and/or receive inappropriate material is prohibited at all times. Inappropriate material includes, but is not necessarily limited to, sexually explicit or racist or discriminatory material, or any other material the MS Society of Canada deems to be inappropriate. Please refer to the Workplace Relationships Policy for further definitions of inappropriate material.

- Information transferred from the ***MS Society*** e-mail address will be treated with the same standards as information on ***MS Society*** letterhead.
- Employees must not send unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam). The creation or mass distribution of e-mail/ newsgroup messages (Spam) outside of the MS Society is prohibited.
- Users must not alter the "From:" line or other attribution-of-origin information in e-mail, messages, or postings. Anonymous or pseudonymous electronic communications are

forbidden. Users must identify themselves honestly and accurately when participating in chat groups, making postings to newsgroups, sending e-mail, or otherwise communicating online.

- Sending large files to multiple recipients raises concerns regarding network bottlenecks and computing resources. Users should keep this activity to a minimum and consider other alternatives such as file compression and/or the use of DVD's or FTP Sites. As a guideline, if the file size is greater than 5 MB and the distribution list is greater than 5 individuals, users must advise the I.T. Department to discuss alternative delivery options.
- Caution should be exercised when sending confidential data via e-mail. Messages can be misdirected or purposely forwarded to other electronic addresses. If you receive a message intended for another person, notify the sender immediately.

3.6 Background Images, Wallpaper and Screen Savers

All computing devices including but not limited to, Laptops, Netbooks, desktop PC's and mobile devices are the property of the MS Society of Canada and part of the workplace, whether they are out of the office or within the office. Therefore, it is necessary to ensure appropriate use for a professional work environment, especially when it comes to background images/wallpaper and screen savers. Computer background images/wallpaper and screen savers must adhere to the following:

- Must be tasteful and non-offensive
- Should not take heavy toll on system resources such as memory
- Should not hinder the MS Society of Canada's ability to support users
- Must not affect system configuration

Note that the MS Society of Canada will not support problems if there have been extreme modifications to the configuration. Only standard screen savers that come with the base operating system or screen savers/wallpaper that may be developed by the MS Society of Canada for its own promotional purposes may be used. Any offensive background images/wallpaper or screen saver should be reported to IT.

3.7 Remote Access

Only users that have a justifiable business reason for remote access will be authorized for that access by the user's manager.

- Remote users must use a user-ID, a password and RSA Token for access.
- Users who work with MS Society information in a home office must understand what security threats exist in their home office environment and take appropriate measures to ensure the security of the information in that environment.
- All of the MS Society policies applicable for in-office operations still apply for home office operations when home equipment is used for MS Society business. This includes, but is not limited to, standards outlined in the Information Technology Security Policy.

- Users who are logged on through remote access must save all data to network directories to ensure it is backed-up. Failure to do so exposes the MS Society to the risk of losing valuable and in some cases essential data.
- Remote control software such as PCAnywhere, Log Me in or Go to My PC is strictly prohibited from use on MS Society computing resources without the express written consent of the Manager, Infrastructure Services.

3.8 Assets

Portable information technology such as laptops, netbooks and mobile devices are entrusted to the user, who is fully accountable for their use and security

- Loss of the device, or unauthorized access, exposes the MS Society to loss of confidential information as well as loss of the physical asset. All losses of MS Society assets must be reported to the help desk immediately.
- Loss or damage to MS Society laptops must be reported immediately and any damage not caused by normal wear and tear may be the responsibility of the user to which they are assigned. This will depend on the circumstances and insurance ramifications.
- Loss or damage to MS Society mobile devices (phones, tablets, etc.) must be reported immediately. Damage not caused by normal wear and tear will be the responsibility of the user to which they are assigned.
- Laptop or Netbook computers used in the office or at a remote locations, must be physically secured by a locking device. Laptop's or Netbook's not in use should be locked and out of sight. You must never use, or allow others to use, the MS Society's portable information technology in violation this Acceptable Use Policy.

3.9 Mobile Devices

It is the responsibility of any employee of the MS Society who is connecting to the organizational network via a mobile (i.e. Blackberry, iPhone, iPad, Android, etc.) device or service to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection and service, used to conduct MS Society business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

- General access to the organizational network through Internet by mobile devices and services through the MS Society network is permitted upon receipt of the Mobile Device Management Agreement signed by the end user.

- Employees and his/her family members using the Internet for recreational purposes through company networks are strictly forbidden

- Employees using corporate issued mobile devices and services will refrain from using any high bandwidth internet based application unless arrangements have been made

with the employee's manager and IT. Any charges incurred that have not been pre-authorized will be the sole responsibility of the employee.

- Employees using corporate issued mobile devices for personal use agree to reimburse the MS Society a personal use monthly fee as referenced in the MS Society of Canada Mobile Device Procedures Document

- All mobile devices used for business interests, whether personal or Society -owned, must display reasonable physical security measures if they are connected to the Society's network. Users are expected to secure and password protect all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried.

- Prior to initial use for connecting to the corporate network, all users must be registered with IT and the Mobile Device Management Agreement must be signed and returned to IT.

- Mobile users agree to immediately report to his/her manager and the Manager, Infrastructure Services or VP of IT any incident or suspected incidents of unauthorized access and/or disclosure of company resources, databases, networks, etc.

- Mobile users also agrees to and accepts that his or her access and/or connection to the MS Society networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

- The MS Society reserves the right to turn off without notice any access port to the network that puts the company's systems, data, users, and clients at risk.

3.10 Virus Management

- Employees are strictly prohibited from introducing malicious programs onto Society's computing resources (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Virus detection software must be installed on each workstation and run at regular time intervals to scan files for possible existence of computer viruses. Employees must not attempt to disable virus protection software. Employees that suspect they have a virus must immediately stop using the computer and contact the help desk
- It is the employee's responsibility to assist in keeping programs of a viral nature off any System. The employee should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these processes.

3.11 Game Playing

Users are permitted to use any game supplied **as part of the base operating system** provided it is:

- on their own time (eg. Coffee breaks, lunch, etc.) and in no way adversely affects their job performance.
- Users are strictly prohibited from installing any games on the MS Society of Canada computers.

3.12 Personal use

MS Society's computing resources are intended for business purposes only. Occasional personal use is permitted; however, authorized individuals must **NOT**:

- Consume computing resources in any way that it may impede on MS Society's business
- Reduce their productivity or interfere with their duties
- Cause the reduction of productivity or interfere with duties of other authorized individuals
- Engage in personal activities that are inappropriate

3.13 Inappropriate personal use activities

The use of the MS Society's computer resources is specifically prohibited for any of the following purposes and any User using the systems for such purposes shall be subject to disciplinary action (or other corrective action for non-employees), including, if appropriate, termination:

- Printing multiple copies of documents
- Playing games
- Downloading executable programs files, or entertainment software
- Downloading executable programs files such as games, shareware or freeware
- Engaging in communication practices that involve ongoing message receipt and transmission, referred to as "instant messaging" that is not endorsed by IT.
- Viewing or listening to streaming video or audio such as radio stations or watching video programs for non-MS Society related activities
- Using Internet services that automatically download information, such as sports scores, stock prices or other continuous data streams, such as Napster (music) or Bit Torrent (videos)
- Sending or receiving messages relating to another business operated by the User for personal gain
- Sending or receiving messages relating to any illegal activities.
- Possession/downloading of copyright material including music, video, and literary material.
- Or otherwise creating unnecessary demand on computing resources

3.14 Safeguarding MS Society data

Data stored on the local computer hard drives is **NOT** backed up and furthermore, is at risk of exposure if the computer is lost or stolen. All users have an obligation to ensure that all MS Society data is stored in safe locations preventing unauthorized access as well as ensuring the data is backed up. Specifically, the following guidelines must be followed:

- All files must be saved in Office 365 to One Drive, Team Sites or Groups
- Do not save files on local computers (C:\, desktop, My Documents, etc.)
- Do not save files on USB drives unless they are immediately transferred to Office 365 and then immediately deleted from the USB drive
- Outlook “archive” files are not permitted due to the 50 GB storage limits applied to all mailboxes

4.0 Sanctions for Misuse

Individuals who misuse equipment of the MS Society of Canada or are non-compliant with the guidelines of this manual will be subject to appropriate corrective or disciplinary measures. These measures may include any of the following:

- Oral reprimand (noted in employee's file)
- Written warning placed in employee's file.
- Loss of computer resource privileges.
- Change of work assignment.
- Suspension
- Demotion
- Termination of employment.

In addition, some violations of policies and procedures in this manual have legal ramifications. Appropriate authorities will be notified if behavior persists.