Technology Use Policy

Version:	1.0
Approved:	June 26th, 2024

Purpose:

The Mycological Society of Toronto owns, maintains and manages Information Technology (IT) resources to support the educational, instructional, and administrative activities of the MST.

This policy sets out the acceptable and responsible use of MST IT Resources, in order to protect the MST and its Members, and to ensure the appropriate use of IT Resources and Information Assets in compliance with privacy law and in accordance with MST policies.

This policy applies to all MST Staff's use of IT Resources. The use of personally-owned equipment that involves the use of IT Resources is also covered by this Policy. This Policy does not affect the rights of MST Staff to their intellectual property stored or transmitted using IT Resources.

Definitions:

Member	A member is an individual who is either the account holder of an individual membership or an individual included in a family membership.
Board	The Board of Directors of the MST.
Director	A member of the Board of Directors of the MST.
Volunteer	A member of the MST acting on behalf of the MST. Includes members and Directors.
Staff	An individual working on behalf of the MST on a volunteer or paid basis.
IT Resources	Information technology resources provided by the MST, whether on premises or hosted remotely. IT Resources include but are not limited to: networks, servers, databases, business systems, websites, computers and computer systems, laptops, storage devices, and online collaborative tools including email and social media sites.
Electronically-Stored Information	MST members' personal electronic information, that is created and communicated in digital form and which is accessible through IT Resources.
Personal Information	According to the Personal Information Protection and Electronic Documents Act in Canada, and for the purposes of this policy, "Personal Information" means information about an identifiable individual (e.g. name, address, email address and telephone number).
Shared Account	An account that can be accessed by multiple MST Staff to accomplish a single shared function, such as supporting the functionality of a process, system, device or application.

References:

- Mission and Values of the MST
- Anti-Harassment Policy
- Code of Conduct Policy
- Membership Policy
- Bylaws: 2.1 - 2.7 (Membership)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Canada's Anti-Spam Legislation (CASL)

Policy:

1. Authorized Use

1.1 MST Staff will:

a. Use IT Resources for which the MST has given express authorization only for intended purpose(s);
b. Take all reasonable steps to avoid compromising the confidentiality, integrity, and availability of IT Resources;
c. Abide by applicable laws and regulations;
d. Abide by applicable MST policies, and;
e. Respect the rights and privacy of other MST Members and those outside of the MST community.

1.2 MST Staff who fail to comply with this Policy will be subject to one or more of the consequences listed in Section 0.
1.3 The MST reserves the right to limit or restrict access to IT Resources by MST Staff based on:

a. institutional priorities;
b. financial considerations;
c. one or more violations of this Policy or other MST policies;
d. contractual agreements; or
e. provincial or federal laws.

2. Limitations on Personal Use by MST Staff

2.1 MST Staff are permitted to use IT Resources for occasional and limited personal use and consistently with this policy.
2.2 The viewing or distribution of harassing, defamatory, discriminatory, pornographic or hateful material and messages by MST Staff using IT Resources is prohibited.
2.3 MST Staff should not store or transmit personal information using the MST's network, equipment, or accounts.

3. Use of MST Email

3.1 MST-provided email accounts must not be considered secure or private.
3.2 MST Staff will not use their personal, educational or employer email accounts for MST correspondence.
3.3 MST Staff will not use MST-provided email accounts for personal communication or when subscribing to personal mailing lists.
3.4 Automatic forwarding of MST email to domains not controlled by the MST is prohibited.
3.5 Sending email from MST-provided email accounts via mail servers in domains not controlled by the MST is prohibited.
3.6 Email transmission of Members' Personal Information to an external email account is prohibited.
3.7 Email is primarily a transactional communication tool and should not be used as a system of record or for long-term storage of files. When appropriate or necessary, emails and/or email attachments should be transitioned to appropriate MST electronic storage systems.

3.8 MST Staff will not delete email necessary for business continuity, either during or upon termination of their term of volunteering and/or employment, including but not limited to:

a. legal correspondence;
b. proprietary or confidential information, and;
c. compliance-related correspondence.

4. Security and Ownership Rights

4.1 MST Staff are required to protect confidential information regarding members and affairs of the MST, including but not limited to:

a. identity of or details about members, except as governed by the Privacy Policy;
b. financial information and records;
c. contracts, and;
d. technical information such as databases, login credentials, passwords and software license keys.

4.2 Login credentials and passwords shall not be shared with any person without the explicit approval of the Board of Directors.
4.3 It is the duty of the Technical Director to change passwords as necessary, and to disseminate login credentials and passwords in a secure manner to authorized persons.
4.4 The Technical Director, the President and the Vice-President shall have access to current login credentials and passwords for all MST Shared Accounts and related tools and services at all times
4.5 Login credentials and passwords for Shared Accounts (i.e. accounts to which multiple MST Staff require access) may only be changed by the Technical Director, the President, or the Vice-President.
4.6 If login credentials and/or passwords for a Shared Account is changed, the new login credentials and/or passwords must be immediately stored in the MST's password escrow in accordance with current procedure.
4.7 Staff have the right to reset or request a reset of passwords for accounts to which they are the only individual requiring access, including their:

a. email account;
b. document repository account;
c. wiki account;
d. password escrow account, and;
e. Slack account.

4.8 MST Staff who have deleted files from one IT Resource, such as a computer hard drive are responsible for managing copies that may continue to exist in or on other IT Resources, such as shared drives. MST Staff are responsible for ensuring file management and disposition of Information Assets in accordance with MST policies and procedures.
4.9 Information Assets created or received outside of IT Resources, such as on a personal smartphone or computer must be stored on MST-controlled IT Resources as soon as possible to ensure continuity during a Staff member's absence.

5. Privacy

5.1 IT Resources are exclusively the property of the MST. The MST respects MST Members' reasonable privacy expectations but MST Members will not have an expectation of complete privacy when using the MST's IT Resources.
5.2 MST Members' privacy rights may be superseded by the MST's right to protect:

a. the integrity of its IT Resources;
b. the rights of other MST Members; or
c. the MST's property.

5.3 The MST reserves the right to monitor and log usage of its IT Resources.

5.4 The MST also reserves the right to examine and preserve material stored on or transmitted through its IT Resources at its sole discretion. Examples of situations where the MST may exercise this right include but are not limited to situations where the MST suspects:

a. this Policy has been violated;
b. any other MST policy has been violated;
c. any federal or provincial law has been violated; or
d. examination is necessary to protect the integrity of its resources.

5.5 The MST will not normally access an MST Member's Electronically-Stored Information without consent except for certain limited and specific circumstances, including but not limited to:

a. investigations regarding security, illegal activity, or activity that may contravene the MST's policies and procedures;
b. compassionate circumstances, as permitted by law;
c. where necessary to carry out urgent operational requirements during an volunteer's absence when alternative arrangements have not been made; and
d. compliance with law or legal obligations.

5.6 Authorized MST Staff or service providers under contract with the MST, who operate and support IT Resources, may access Electronically-Stored Information without notice to MST Members in order:

a. to address emergency problems;
b. to perform routine system maintenance; or
c. for any other purpose required to maintain the integrity, security and availability of the IT Resources.

5.7 In the process of monitoring IT Resources, the MST will:

a. use all reasonable efforts to limit access to MST Members' Electronically-Stored Information; and
b. not disclose or otherwise use any MST Members' Electronically-Stored Information that has been accessed, except in accordance with the applicable MST policies, procedures and guidelines, and as permitted or required by law.

5.8 If the MST is required to disclose a MST Member's Electronically-Stored Information, in accordance with the law, such disclosure will be reviewed and approved by the Board of Directors, prior to the release of the Electronically-Stored Information.

6. Specific Violations

6.1 Unauthorized Use. Violations of Section 1.1.a include, but are not limited to:

a. using IT Resources without specific authorization where specific authorization is required;
b. using another person's electronic identity, password or log-in credentials for IT Resources;
c. accessing files, data or processes without authorization;
d. using IT Resources to hide a persons' actual identity;
e. using IT Resources to interfere with other systems or persons;
f. using IT Resources to harass or stalk another person or entity;
g. sending threats, "hoax" messages, chain letters, or phishing;
h. intercepting, monitoring, or retrieving any network communication without authorization; or
i. circumventing or attempting to circumvent security mechanisms.

6.2 Breach of Confidentiality, Integrity and Availability of IT Resources. Violations of Section 1.1.b include, but are not limited to:

a. obtaining or using someone else's password or other authentication credentials for IT Resources;
b. disclosing a personal password or other authentication credentials for IT Resources;
c. permitting other MST Staff to access or use their account(s) provided by the MST;
d. propagating computer viruses, worms, Trojan Horses, malware or any other malicious code;
e. preventing others from accessing an authorized service;
f. spreading material that supports bulk mail, junk mail, or spamming;
g. degrading or attempting to degrade performance or deny service; or
h. corrupting, altering, destroying, or misusing data or information.

6.3 Unlawful Use. Violations of Section 1.1.c include, but are not limited to, using or attempting to use IT Resources to:

a. pirate software;
b. access material that is illegal, or that advocates or facilitates illegal acts;
c. download, install, use, stream, or distribute unlawfully or illegally obtained media (e.g., software, music, movies);
d. override, remove or pause any security software installed on IT Resources by the MST or at its direction;
e. access technology that is considered a controlled good under federal law on an unencrypted connection;
f. commit criminal harassment, hate crimes, or libel and defamation;
g. commit theft or fraud; or
h. violate child pornography criminal laws.

6.4 Breach of MST policies. Violations of Section 1.1.d include, but are not limited to, using or attempting to use IT Resources to:

a. engage in discrimination and harassment, including making threats, stalking, or distributing malicious material; or
b. direct others to breach any provision of this policy.

6.5 Breach of Privacy. Violations of Section 1.1.e include, but are not limited to:

a. accessing, attempting to access, or copying another person's Electronically-Stored Information without authorization; or:
b. divulging sensitive personal data to which certain MST Staff have access concerning Members and/or Staff without a valid and lawful administrative reason.

7. Reporting

7.1 MST Staff are responsible for guarding against misuse or abuse of IT Resources.
7.2 MST Staff will promptly report any known or suspected misuse of IT Resources or violation of this Policy to the Technical Director.

8. Investigation

8.1 Reports of conduct by MST Staff in contravention of this Policy will be addressed by the following means:

- Harassment, violence or discrimination will be investigated under the Anti-Harassment Policy.
- Other violations can be addressed under the Code of Conduct Policy.

8.2 Reports of conduct by MST Staff in contravention of this Policy not addressed by another policy will be addressed by the Board of Directors.

9. Consequences

9.1 Members who violate this Policy or any other MST policy may be subject to disciplinary action up to and including, but not limited to:

a. suspension of access to some or all IT Resources;
b. termination of membership in accordance with the Membership Policy and Bylaws; and
c. legal action.

10. Relevant Legislation

10.1 Canada's Anti-Spam Legislation (CASL)
10.2 Personal Information Protection and Electronic Documents Act (PIPEDA)