STAFF AND HUMAN RESOURCES POLICY
5.0

Policy Title: **Acceptable Use**

Last Approved: **October 2023**

BACKGROUND

The purpose of this policy is to guide Association employees in the use of Association computers and other equipment and resources including but not restricted to laptops, telephones, cellular phones, Personal Data Devices (PDA) units and all other devices which have access to or may store information obtained from the Association's computer networks (hereinafter collectively referred to as "the computer network").

APPLICATION

This policy applies to all Association employees.

POLICY STATEMENT

Employees of the Association shall comply with this policy and any related guidelines and directives to enable reasonable and appropriate use of the computer network and all Association resources.

5.1 ACCEPTABLE USE

Acceptable uses of the computer network include, but are not limited to, the following:

- Purposes related to the specific functions of each employee's job or purposes required to assist employees in carrying out the duties of their employment;
- Reasonable private purposes which are consistent with this policy; and
- Work-related purposes
    a. Unless specifically directed otherwise an employee may use the computer network if access to the computer network is required to perform any portion of work duties assigned to the employee.
    b. All work related uses must be in accordance with the terms of this policy.
- Incidental Purposes
    a. Employees may also use the computer network for reasonable private purposes such as sending and receiving personal messages as long as such usage does not interfere with the duties of employment.
    b. Employees shall comply with the following rules in any incidental use of Association resources:
        - Incidental use must not impede the employee's work or the work of others, or affect the Association's ability to carry out its work;
        - For incidental use, each employee shall reimburse the Association for all costs incurred by the employee's incidental use (i.e. photcopying personal documents; long distance calls on Association cell phone) by submitting a Personal Use Form to Corporate Services (see 5.0-A Personal Use Form).

5.2 UNACCEPTABLE USE

Unacceptable uses of the computer network include, but are not limited to, the following:

- Any use by an employee that interferes with the duties of employment;
- Any use by an employee that exposes the Association to cost or risk of liability; and
- Unauthorized release of information:
    a. Giving out personal information about another person.
    b. Providing information about, or lists of employees to outside parties.
    c. Providing confidential information about the Association or its operations to outside parties.
- Unauthorized personal use:
    a. Use of the Association's name, computers or other equipment for personal business or commercial or for-profit purposes.
    b. Downloading entertainment software (e.g. Music, videos, etc.) or other files not related to objectives of the Association for transfer to a user's home computer, personal computer, or other media.
- Misuse of Passwords:
    a. Revealing a password to any unauthorized person.
    b. Allowing use of employee's account by an unauthorized party when work is being done at home.
    c. Circumventing user authentication or security of any host, network or account.
    d. Misrepresenting other users on the network.
- Unauthorized use or modification of equipment or software:
    a. Intentionally modifying or damaging any Association hardware, software, files, mailbox, web page, other data, or passwords belonging to other users.
    b. Unauthorized installation of software, including shareware and freeware.
    c. Any activity that uses significant bandwidth unless specifically authorized by the network administrator.
    d. Effecting security breaches or disruptions of network communication, including but not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Improper, objectionable or unethical actions:
    a. Using Association computers or other resources for offensive activities such as circulating hate mail, chain letters, harassment, discriminatory remarks, making threats, abusive actions, and other antisocial behaviours, or violation of applicable privacy legislation.
    b. Use of the computer network to access or process pornographic material or other inappropriate text files.
    c. Use of the computer network to access files dangerous to the integrity of the local area network or knowingly subjecting the Association computers, network, or other resources to spam, spoofing, hijacking, and cyber attacks etc.

d. Sending forged or anonymous e-mail or postings.

- Misuse of Copyright:

a. Downloading, copying, or otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner, except when permitted for educational purposes.

b. Installation or distribution of products that are not appropriately licensed for use by the Association.

Employees who have questions as to whether a particular activity or use is acceptable should seek further guidance from Corporate Services, the Executive Director, or their Director.

5.3 MONITORING

- The computer network is owned by the Association and the Association reserves the right to access contents of all files stored on the network and all messages transmitted through its computer network.
- The Association keeps and may monitor logs of usage of equipment which may reveal information such as:

a. Internet sites that have been accessed by employees.

b. Email addresses of those with whom employees have communicated.

c. The content of communications including emails and instant messages.

- Except as otherwise provided for in this policy, the Association:

a. Will not engage in real-time surveillance of internet or equipment usage.

b. Will not disclose any of the logged, or otherwise collected, information to a third party except under compulsion of law.

- In cases where information is accessed the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary.
- Employees are advised that any matter created, received, stored in or sent from the Association's network or email system is not necessarily private and all material is subject to applicable privacy legislation. The Executive Director or designate reserves the right to access any file, data, or information to determine whether or not an employee is utilizing the network or email system appropriately and within the guidelines of this policy.

5.4 WEB PAGES

Each department will ensure that information they want posted to the internet meets the following minimum standards:

- Sources must be cited.
- Information should be as correct and timely as possible.
- Copyright laws apply and copyright notices must be included where appropriate.
- Privacy consideration should be addressed.
- Material published to the Association website must have appropriate approvals by the Executive Director prior to posting.

5.5 COPYRIGHT

- Hardware and software must only be used legally in accordance with both the letter and spirit of relevant licensing and copyright agreements.

5.6 SECURITY

- Confidential information should always be treated in a secure manner appropriate to the media. Association cell phones and laptops should be locked when not in use and not left alone unattended.
- Every employee must immediately report any possible or suspected breach of security to their Director who in turn shall immediately notify the Director of Corporate Services.

5.7 USERNAMES AND PASSWORDS

- Employees who require computer network access in order to perform the functions of their employment will be assigned usernames and passwords in order to be able to access required services. Passwords are not to be shared.

5.8 HARDWARE AND SOFTWARE

- All purchases must be approved by the Director.
- Permission from Corporate Services must be obtained before any software (including public domain software) is installed on any Association computer.
- Hardware and software must only be used legally in accordance with both the letter and spirit of relevant licensing and copyright agreements.

5.9 REMOTE ACCESS

- The Association provides for all employees to access their email and network information remotely and employees are strongly encouraged to use this resource to reduce the chances of confidential data being lost or stolen on a laptop. Employees are permitted to use remote access to the Association computer network subject to the following:
  a. Access must be strictly controlled, using password authentication;
  b. It is the responsibility of employees with remote access privileges to ensure that a connection to the Association is not used by non-employees to gain access to Association computer network resources; and
  c. The employee must take every reasonable measure to protect the Association's assets and information.

5.10 ENFORCEMENT

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- When there are reasonable and probable grounds to believe that a user has used the computing technology, networks, and/or online services for criminal or illegal purposes, the breach will be reported to the appropriate authorities.

REFERENCES