SPORT FOR LIFE SOCIETY POLICY

POLICY TITLE: INFORMATION TECHNOLOGY	
Date Created: November 25, 2015 Date Approved: February 2026 Review Frequency: Annual	Number of Pages: 7

TABLE OF CONTENTS

1. PURPOSE

1.1. This Information Technology (IT) Policy ensures the effective and secure use of information technology resources (IT Resources) at Sport for Life Society (the “Society”). It aims to protect the integrity, confidentiality, and availability of the Society’s IT systems and data, ensuring that they are used in a manner that supports the Society's mission and complies with applicable laws and regulations. To this end, this policy aims to safeguard the security of all the Society’s IT Resources by establishing the Society's responsibilities in the use of these resources.

2. SCOPE

2.1. This policy applies to all the Society's Representatives and authorized users who have been granted permission to use the Society’s IT Resources.

3. DEFINITIONS

3.1. **Representative(s) -** Any individual elected, acclaimed, or appointed by Sport for Life Society (the "Society"), or engaged under an executed written agreement with the Society as an employee, volunteer, or independent contractor to provide services on behalf of Sport for Life.

3.2. **Artificial Intelligence ("AI") -** A machine-based system that can, for a given set of human-defined objectives, make predictions, summaries, recommendations, or decisions influencing real or virtual environments. (Source: NIST)

3.3. **Authorized User** – Any individual employed by, or engaged in activities, on behalf of the Society, including employees, contractors, volunteers, researchers, Board members, committee members, administrators, guests, or other individuals who have been granted permission to access certain data or systems that are part of the Society's IT Resources by virtue of their role and responsibilities.

3.4. **Availability** – The assurance of timely and reliable access to the Society's IT Resources for their intended use.

3.5. **Confidentiality** – The assurance that IT Credentials or Data can only be accessed by Authorized Users or authorized systems.

3.6. **Confidential Data** – Information whose protection and use is mandated and governed by law, regulation, industry requirement, contract or any of the Society's regulation, policy or directive because of its sensitive nature, including, but not limited to, personal information.

3.7. **Cybersecurity** – To protect the Society's digital assets and data from cyber threats and ensure confidentiality, integrity, and availability.

3.8. **Data** – Digital information stored in or transmitted through the Society's IT Resources and includes documents, files, databases, websites, e-mails, chat messages, and multimedia.

3.9. **Generative Artificial Intelligence (AI) -** The class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content. (Source: NIST)

3.10. **Information Technology Credentials** ("IT Credentials") – A proof of identity used to control access to the Society's IT Resources, including, but not limited to, usernames, passwords and digital certificates.

3.11. **Information Technology Resources** ("IT resources") – All the Society-owned or provisioned IT assets. This includes, but is not limited to, Data, cloud services, software, hardware, voice communications systems, Internet of Things (IoT), devices, artificial intelligence technologies, photos, and the services that utilize any of these IT resources.

3.12. **Integrity** – The assurance of the accuracy and consistency of Data and that Data is not altered by unauthorized users.

4. APPLICATION

4.1. This IT policy ensures that the Society provides guidance for the appropriate use of technology and information systems within the organization. This policy applies to Authorized Users on behalf of the Society. This policy applies to all IT resources regardless of the time of day, location, or method of access, including working from home or remotely.

4.2. All Representatives, including Authorized Users, will be informed annually of this policy, which emphasizes that their compliance is expected at all times and in all locations. Their intentional and inappropriate use of the Society's IT resources may result in disciplinary action, up to and including dismissal.

4.3. The Society's Representatives are expected to bring their own devices and personal computing devices. Employees may have a mix of Bring Your Own Device (BYOD), Personal Computing Devices (PCD), and the Society's owned devices. This Policy is written to cover all Authorized Users.

4.4. The Society's IT Resources are provided to Authorized Users only to advance the Society's mission and support related administrative, financial, and operational activities, including projects and services.

4.5. Authorized Users shall use the Society's IT Resources, for the purposes provided in 4.4 above, and in a responsible, ethical, and lawful manner, in accordance with the Society's policies and procedures, and other relevant the Society's standards and IT policy, and in compliance with applicable laws and regulations as well as, in certain circumstances, the Society's contracts and agreements.

4.6. Authorized Users shall respect the intellectual property rights of others.

4.7. Authorized Users have a reasonable expectation of privacy in their use of the Society's IT Resources.

4.8. Authorized Users shall take reasonable and prudent steps to protect the Security and ensure the Confidentiality, Integrity, and Availability of the Society's IT Resources. This includes social media and all forms of communication, as further outlined in the Sport for Life's IT Procedures.

4.9. The ability to access and use the Society's IT Resources does not, by itself, imply authorization to do so. Authorized Users must use technology in accordance with IT documents and best practices in the business of Sport for Life.

5. ACCEPTABLE USE

5.1. **Authorized Access:** IT resources, including computers, networks, software, and data, should only be used for purposes related to the Society's mission and activities.

5.2. **Personal Use:** Limited personal use of IT resources is permitted if it does not interfere with work responsibilities or violate any terms of this policy. These include, but are not limited to, your home's Internet/networking system, personal devices (mobile phones, tablets, computers), and AI technologies.

5.3. **Communication Standards**: All the Society's Representatives are to comply with Sport for Life's *Social Media Guidelines* and *Sport for Life's IT Procedures' Social Media and Communications* section.

5.4. **Prohibited Activities:** The following activities are prohibited:

i. Unauthorized access to, or modification of, any IT resources and data.

ii. Installations of any unauthorized software and hardware that are not approved by the IT Manager.
iii. Distribution of malicious software or engaging in activities that may harm the Society's IT infrastructure.
iv. Viewing, downloading, or distributing inappropriate or illegal content.

6. WORK FROM HOME AND REMOTE WORK

6.1. Each of the Society's Representatives plays a vital role in maintaining the security and privacy of the Society's information from anywhere at any time. They must adhere to this IT Policy to protect the Society's data and equipment.

6.2. Each of the Society's Representatives must ensure Wi-Fi is secure and remain vigilant for suspicious activity. They must also use secure connections (e.g., VPNs) for remote access while working in public locations and/or using public WiFi connections.

6.3. All data must be handled securely, and any suspected security threats or data breaches must be reported to the Society's IT team immediately.

7. DATA PROTECTION AND PRIVACY

7.1. **Confidentiality**: All sensitive or confidential information must be protected from unauthorized access. This includes client data, financial information, and personal employee details. The Society's Representatives must handle sensitive information with care and must not share or disclose confidential data without proper authorization.

7.2. **Data Handling/Management:** Data should be stored securely, encrypted where necessary, and shared only with authorized users when required. This includes the management of the cloud and local storage.

7.3. **Data Backup:** Regularly back up important data and ensure backups are stored securely. Data backup procedures should be in place, and Authorized Users will regularly test to ensure their functionality and effectiveness.

7.4. **Data Retention:** Data should be retained only as long as necessary for business purposes, in accordance with relevant regulations, and in compliance with organizational guidelines.

7.5. **Data Destruction:** Data must be securely disposed of after a specified period, in accordance with applicable Canadian standards and regulations.

8. SECURITY AND CYBERSECURITY MEASURES

8.1. **Internet Use:** Use the internet responsibly. Avoid accessing inappropriate or non-work-related sites that could pose security risks.

8.2. **Email:** Be cautious with email attachments and links. Avoid opening emails from unknown or suspicious sources. Notify the IT Manager immediately of any suspicious emails.

8.3. **Mobile and Computing Device Security:** Ensure mobile and computing devices are secured with passwords or biometric authentication. This includes personal devices if they are connected to the Society's IT resources. Report lost or stolen devices to the IT Manager immediately.

8.4. **IT Credentials/Password Management:** Strong passwords must be used and changed regularly. The Society has Shared Accounts, for which password sharing may be required only for Authorized Users. Refer to *Sport for Life's IT Procedures' Shared Accounts* section for detailed procedures.

8.5. **Network Security:** Ensure that firewalls, antivirus software, and other security measures are in place and regularly updated to protect the network from threats. Utilize firewalls, secure Wi-Fi, and network monitoring tools to safeguard against unauthorized access and detect suspicious activities. Use secure connections (e.g., VPNs) for remote access, including public WiFi access.

8.6. **Incident Reporting:** Immediately report any cybersecurity incidents, IT security incidents, or issues to Sport for Life's IT Manager and ensure a response is acknowledged. This includes data breaches, system outages, or suspicious activities. Follow the Society's incident response plan for managing and mitigating incidents, as outlined in the One Stop Smartsheet: Liability Claim form
The Cyber Breach Response Hotline is available 24/7 at 1-800-607-1355 (toll-free).
Refer to *Sport for Life's IT Procedures' Cybersecurity and IT Incident Response Plan* for the detailed outline.

9. ARTIFICIAL INTELLIGENCE TECHNOLOGIES

9.1. All Society Representatives, including Authorized Users, must comply with Sport for Life's IT Policy—particularly Section 7.1—when using AI technologies. Users are responsible for managing emerging risks associated with these tools at all times.

9.2. Users must protect their personal information and the Society's confidential information. Such information **must not** be entered into any AI technologies, including but not limited to ChatGPT, OpenAI services, Microsoft Copilot, and Google Gemini.

9.3. Generative AI may be used to create written or visual content, provided that the content aligns with the Society's strategic plan, language guidelines, branding standards, and other relevant policies, including the Social Media Guidelines and IT Procedures. **All AI-generated content must be reviewed and edited by a human before being shared externally.**

9.4. Any citations or factual information provided by AI must be verified by a human for accuracy and reliability. Citations must be properly formatted according to the *Sport for Life's Language and Style Guide*.

9.5. AI Notetakers

9.5.1. **Authorized AI Notetaking Software:** Sport for Life Representatives may use IT-approved AI notetakers, including Fathom, Read.ai, and Zoom AI Companion.

9.5.2. **Consent Required:** All participants must be informed and give consent before any recording or transcription. If one participant declines, the AI notetaker must not be used.

9.5.3. **Confidentiality:** AI notetakers must not be used for highly sensitive meetings (e.g., HR, legal, disciplinary, confidential client matters). Personal and Sport for Life confidential information must not be unnecessarily captured.

9.5.4. **Review and Storage:** All AI-generated transcripts and summaries must be reviewed by a human before being shared or treated as official records.

9.5.5. **Retention and Security:** AI outputs must follow Sport for Life's Data Retention and Destruction procedures. Access must be limited to authorized users, and MFA must be enabled where available.

9.6. **No exceptions apply. All Society Representatives, including Authorized Users, are accountable for complying with these requirements. Misuse, non-compliance, or unauthorized use of AI technologies is not permitted under any circumstances.**

10. EQUIPMENT AND SOFTWARE

10.1. **Usage:** All IT equipment and software provided by the Society should be used responsibly and maintained in good condition. Take proper care of all IT equipment (e.g., ensure keyboard buttons are not missing, screens are not loose, siding panels are not loose, and cables are not damaged). Report any missing/damaged parts, malfunctions, or issues to the Society's IT team promptly. If users are found at fault prematurely, the replacement and repair costs may be at their expense.

10.2. **Software Licenses:** Only licensed software may be installed on the Society's computers. Unauthorized software or pirated copies are prohibited and can pose security risks.

10.3. **Updates:** To protect against vulnerabilities, keep software and operating systems up to date with the latest patches and updates.

10.4. **Life cycle:** Society Representatives are provided with and have access to IT equipment for the expected lifespan of the equipment. The Society will replace them as needed. Refer to the *IT Procedure's Computer Hardware* section.

10.5. **Return of Equipment:** Upon termination of employment or engagement, all Society-owned equipment must be promptly returned clean and in working order, with all cables and accessories fully intact.

For more detailed information, refer to *Sport for Life's IT Procedures*.

11. TRAINING AND AWARENESS

11.1. **Training:** The Society's Representatives will receive training on IT security best practices and this policy as part of their orientation and ongoing professional development. They will also participate in cybersecurity training to recognize and respond to threats such as phishing and social engineering attacks.

11.2. **Updates:** This policy will be reviewed and updated regularly to reflect changes in technology and organizational needs. All personnel will be notified of significant updates.

12. COMPLIANCE AND ENFORCEMENT

12.1. **Compliance:** All the Society's Representatives, including Authorized Users, must comply with this policy. Failure to do so may result in disciplinary action, up to and including termination of employment or engagement with the Society.

12.2. **Review:** This policy will be reviewed annually or as needed to ensure its effectiveness and compliance with relevant laws and regulations.