Sport for Life

SPORT FOR LIFE SOCIETY POLICY

POLICY TITLE: INFORMATION TECHNOLOGY	
Date Created: November 25, 2015 Date of Last Review: September 2024 Date Approved: February 2025	Number of Pages: 5

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. It aims to protect the integrity, confidentiality, and availability of Sport for Life's IT systems and data, ensuring that they are used in a manner that supports Sport for Life's mission and complies with applicable laws and regulations. To this effect, this policy aims to safeguard the security of all Sport for Life's IT Resources, by establishing the responsibilities of Sport for Life in the use of all Sport for Life's IT Resources.

2. SCOPE

2.1. This policy applies to all Sport for Life Representatives and authorized users who have been granted permission to use Sport for Life's IT Resources.

3. DEFINITIONS

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

3.2. **Authorized User** – Any individual employed by, or engaged in activities, on behalf of Sport for Life 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 Sport for Life's IT Resources by virtue of their role and responsibilities.

3.3. **Availability** – The assurance of timely and reliable access to Sport for Life IT Resources for their intended use.

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

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

3.6. **Cybersecurity** – To protect Sport for Life's digital assets and data from cyber threats and ensure confidentiality, integrity, and availability.

3.7. **Data** – Digital information stored in or transmitted through Sport for Life IT Resources and includes documents, files, databases, websites, e-mails and multimedia.

3.8. **Information Technology Credentials** ("IT Credentials") – A proof of identity used to control access to Sport for Life IT Resources, including, but not limited to, usernames, passwords and digital certificates.

3.9. **Information Technology Resources** ("IT resources") – All Sport for Life-owned or provisioned IT assets. This includes, but is not limited to, Data, cloud services, software, hardware, voice communications systems, internet of things (IoT) and devices, and the services that make use of any of these IT resources.

3.10. **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 Sport for Life Society provides guidance for the appropriate use of technology and information systems within the organization. This policy applies to Authorized Users on behalf of Sport for Life 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 Sport for Life Representatives, including Authorized Users, will be made aware of this policy annually, that their compliance is expected, and that their intentional, inappropriate use of Sport for Life IT resources may result in disciplinary action up to and including dismissal.

4.3. Sport for Life contractors 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 Sport for Life Society-owned devices. This Policy is written to cover all Authorized Users.

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

4.5. Authorized Users shall use Sport for Life's IT Resources, for the purposes provided in #4.4 above, and in a responsible, ethical, and lawful manner, in accordance with Sport for Life's policies and procedures, and other relevant Sport for Life's standards and IT policy, and in compliance with applicable laws and regulations as well as, in certain circumstances, Sport for Life'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 Sport for Life'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 Sport for Life'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 Sport for Life'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. WORK FROM HOME AND REMOTE WORK

5.1. Each Sport for Life representative plays a vital role in maintaining the security and privacy of Sport for Life's information from anywhere at any time. They must adhere to this IT Policy to protect Sport for Life's information and equipment.

5.2. All data must be handled securely, and any suspected security threats or data breaches must be reported to Sport for Life's IT team immediately.

6. ACCEPTABLE USE

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

6.2. **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.

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

i. Unauthorized access to, or modification of, any IT resources or data.
ii. Installation of unauthorized software or hardware.
iii. Distribution of malicious software or engaging in activities that may harm Sport for Life's IT infrastructure.
iv. Viewing, downloading, or distributing inappropriate or illegal content.

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. Sport for Life Representatives must handle sensitive information with care, and not share or disclose confidential data without proper authorization.

7.2. **Data Handling/Management:** Data should be stored securely, encrypted where appropriate, and only shared with authorized users. Data backup procedures should be in place and regularly tested. This includes cloud and storage management.

7.3. **Data Backup:** Regularly back up important data and ensure backups are stored securely.

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

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 of suspicious emails immediately.

8.3. **Mobile Device Security:** Ensure mobile devices are secured with passwords or biometric authentication. Report lost or stolen devices immediately to the IT Manager.

8.4. **IT Credentials/Password Management:** Strong passwords must be used and changed regularly. The sharing of passwords is strictly prohibited.

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.

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 Sport for Life's incident response plan for managing and mitigating incidents found on the One Stop smartsheet. Liability Claim form
The Cyber Breach Response Hotline is 1-800-607-1355 (available 24/7 toll free).

9. EQUIPMENT AND SOFTWARE

9.1. **Usage:** All IT equipment and software provided by Sport for Life should be used responsibly and maintained in good condition. Take proper care of all IT equipment (e.g., no missing keyboard buttons, loose screens, loose siding panels, damaged cables). Report any missing/damaged parts, malfunctions, or issues to Sport for Life's IT team promptly.

9.2. **Software Licenses:** Only licensed software may be installed on Sport for Life computers. Unauthorized software or pirated copies are prohibited and can pose security risks.

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

9.4. **Return of Equipment:** Upon termination of employment or engagement, all Sport for Life-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*.

10. Training and Awareness

10.1. **Training:** Sport for Life 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.

10.2. **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.

11. Compliance and Enforcement

11.1. **Compliance:** All Sport for Life 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 Sport for Life.

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