SE Data Security Policy

1. Introduction

This policy sets out how anyone permitted to access Snowsport England (SE) data or charged with handling such data must protect that data. Any breach of this policy may put SE in breach of the General Data Protection Regulations and it could result in serious consequences for the organisation. Everyone must therefore read, understand and adhere to this policy at all times.
This policy is designed to cater for both people who are provided with devices by SE to process personal data for SE and people who chose to utilise their own devices to process personal data on behalf of SE.

2. Safeguard Data Privacy

Employees and volunteers must read the Company' Employee and volunteer Data Protection Notice (DPN) and understand that the contents of the DPN is a pledge to colleagues, staff and SE members that SE will protect their information. Data should only be used in ways that will keep customer identity and the confidentiality of information secure. SE must conform to all applicable laws and regulations and employees and volunteers are expected to do so at all times.

3. Password Management

Employees and volunteers are expected to prevent unauthorised access to their Personal Computers with passwords. In general, password complexity should be established according to the job functions and data security requirements. For banking and financial transactions and for restricted access to sensitive personal data passwords should not be shared.

3.1 Password Complexity

To create a strong password, use eight characters or more in an alphanumeric combination, upper and lower case combinations or symbols. You should avoid using complete words. Make your passwords cryptic so they cannot be easily guessed but be sure it is something you can remember. To find the right balance between convenience to remember and difficulty for hackers, consider creating a unique acronym for a sentence or phrase you like or including phonetic or alphanumeric replacements for wording within the phrase. Avoid using personal information such as your name, birthdates, family or pet's names or your company's name in your passwords. Once you have created your strong password, you need to ensure it remains an effective line of defence. To keep your password strong: Never share your passwords with anyone. That includes co-workers, family members and friends.

Choose different passwords for all your accounts. Using the same password for each account is like using the same key to unlock your office, home and car —each site is vulnerable if the wrong person gains access to one.

4. Internet Usage:

Most people use the internet without a thought to the harm that can ensue. SE employees misuse of the internet can place SE in an awkward, embarrassing or even illegal, position. SE provides many employees with personal computers, and these should only be used for accessing internet sites that are related to SE employment. Access to gambling, pornographic and gaming sites with SE owned computers or infrastructure is forbidden.

5. Email Usage for Personal data:

Data breaches can result from misuse of email, and this can result in loss or theft of data and the accidental downloading of viruses or other malware. The transmission of bulk personal data by email is only permitted when that data is included as a file attachment and that attachment is password protected. Any covering email sent with the password protected and encrypted file attached should NOT contain detail of the password protecting that file. The password would ideally be SMS'd to the recipient rather than being sent by email.

6. Mobile Devices including laptops, tablets and phones:

Loss of mobile devices and storage devices poses a real risk of serious breaches of SE personal data integrity. The risk can be reduced in a variety of ways. Anyone who has access to SE data from a mobile device, whether provided by SE or provided by yourself, should take the following steps to reduce the risk of breaches to SE data integrity.

6.1 Physical security of the device

Always keep your device as secure as possible. Do not take it from the office or home unless you need to and when you do look after it in the most secure manner possible. Use hotel safes if they are provided. Do not leave devices unattended or even bags unattended with devices in them. If you have to leave a device in someone else's charge, e.g. a hotel concierge, then make sure that the device is switched off and password protected at start up.

6.2 Do not store personal data on a device

Unless there is a business need to store personal data on a mobile device then personal data should not be kept on that device.

6.3 Ensure barriers to access to any device

All mobile devices should be password protected or have bio protection enabled at start up. If the hardware is capable of supporting disk encryption, such as bitlocker, then this feature should be enabled.

7. Installation of Software, Copyright and Licensing:

Compliance with software copyright and licensing agreements is mandatory on all SE owned devices and is highly recommended for any other device that contains SE personal data. Employees should not download and use software that has not been reviewed and approved by the SE.

8. Virus checking software

SE owned devices should run appropriate virus checking software. This software should update itself with new virus scanning software when new releases become available. This software should be left in protection mode at all times. Any failure of this software should be reported to SE immediately.

9. Technology storage infrastructure SE provides many staff and some volunteers with access to One Drive for business. This has within it a secure file storage system. SE personal data should be stored within One Drive for business in all cases where that system is provided to SE staff, consultants or volunteers. Other storage systems such as Google should not be utilised for SE Personal data if people are provided with access to One Drive for business by SE.

10.Paper records

SE has worked hard to "dematerialise" the data that it uses to run the business, we discourage the use of printed records and store all that we can within our technology infrastructure. Nevertheless, sometimes employees, volunteers, Directors and others may make paper copies of personal data. Paper records should be treated with more care than mobile devices. They should only be taken off SE premises when there is a fundament business need to do so.

11.Reporting Possible Breaches and Security Incidents:

Any person who utilises SE personal data should report any suspicion of a breach of integrity of that personal data the moment that the suspicion arises. They should report the matter to the CEO via email and/or SMS with as much detail as they are able to provide. The CEO will then assemble a group of people to explore the loss, understand the implications of the loss and take the appropriate action. There are very many possibilities for breaching the integrity of SE's protection of personal data but examples would include:

• Loss of a mobile device with personal data on it

• Loss of a memory stick or card with personal data on it

• Loss of a password that provides access to online systems with SE personal data on them

• Sending a file with personal data in it to the wrong email address

• Alteration of personal data without the permission of the owner of that personal data

• Loss of a paper file containing Anything that affects the confidentiality, integrity or availability of personal data must be reported.

Produced By:	Date:	Board Approved:	Review Date:
Snowsport England	Mar 23	Mar 23	Mar 26