Information Security Policy

CONTENTS

1. INTRODUCTION

1.1 Information about our members and work related to the aims of the charity is an important asset to the Society for Back Pain Research (SBPR) and as such we must ensure that this information is kept safe and used appropriately. We have therefore developed this Information Security Policy that complies with relevant legislative requirements to assure our stakeholders that data held and processed by the SBPR is treated with the highest respect and appropriate standards to keep it safe and secure.

1.2 All those working on behalf of SBPR are required to comply with this policy to ensure that the risk of losing data, leaking data and breaching data protection legislation is avoided.

2. SCOPE OF POLICY

2.1 This policy is applicable to, and will be communicated to, all members of the SBPR Executive Committee, other authorised users of the SBPR and third parties who interact with information held by the SBPR and the information systems used to store and process it.

2.2 This policy shall apply to:

a) All information systems (including such as computer equipment, mobile devices, network equipment and telecommunications equipment) owned or operated by SBPR and used to store information.

b) All software installed on applicable information systems by the SBPR.

c) All information stored in the SBPR's information systems.

2.3 Information security shall include protection of the following:

a) Confidentiality: Ensuring that information and systems are accessible only to authorised users.

b) Integrity: Safeguarding the accuracy and completeness of information and processing methods.

c) Availability: Ensuring that authorised users have access to information and systems when required.

3. POLICY OBJECTIVES

3.1 The objectives of this policy are to:

a) Provide a framework for establishing suitable levels of information security for all SBPR information systems (including but not limited to all computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

b) Ensure that all users are aware of and comply with all current and relevant UK and EU legislation related to Information Security.

c) Provide the principles by which a safe and secure information systems working environment can be established for staff, students and other authorised users.

d) Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

e) Safeguard the SBPR from liability or damage through loss or breach of data.

f) Maintain research data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.

4. The SBPR's Approach to Information Security

4.1 The SBPR will use all reasonable, appropriate, practical, and cost-effective measures to protect its information systems and achieve its security objectives.

5. Information Security Responsibilities

5.1 All users of SBPR information systems are responsible for protecting information assets (see Appendix A: SBPR Information Security Checklist and infographic).

5.2 Users must at all times act in a responsible, professional, ethical and security conscious way, maintaining an awareness of and conformance with the security policy.

5.3 The SBPR's Executive Committee is responsible and accountable for ensuring that the objectives of this policy are met.

5.4 Users should report any breach in information security or suspected breach to Deb McStrafick, the Data Protection Officer (contact@sbpr.info) and Secretary of the Society in accordance with the Data Security Breach Management Policy.

6. Policy Awareness

6.1 The Society Secretary and Executive Assistant will publicise this policy and any associated standards and guidelines to all SBPR executive committee members.

7. Monitoring of Information Systems

7.1 The Executive Assistant will monitor SBPR's website, and emails with members and others associated with the work of SBPR to detect unauthorised activity, identify potential weaknesses and pro-actively prevent security incidents (such as phishing emails or website problems).

7.2 This policy and compliance with it applies to all Executive Committee Members users and those who use the SBPR's information systems.

8. Information Security Principles

8.1 The following Information Security Principles govern the security and management of information at the SBPR:

a) Information should be classified according to an appropriate level of confidentiality, integrity and availability in line with our Information Asset Classification System and in accordance with relevant legislation.

b) Those working on behalf of SBPR and involved in information management (see Information Security Responsibilities) must:

a. Handle that information in accordance with its classification level.

b. Comply with any policies, procedures or systems for meeting those responsibilities.

c) Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.

d) Information will be protected against unauthorised access and processing in accordance with its classification level.

e) All data breaches must be reported in line with the Data Security Breach Management Policy.

f) Information security and related policies shall be reviewed biannually by the Executive Committee.

9. Information Asset Classification System

9.1 Table 1 defines the information classification system used by the SBPR to classify the security level of information the SBPR processes. This system aligns with the above Information Security Principles, incorporates the definitions of Personal Data and Special Categories of Personal Data as defined by the EU General Data Protection Regulation (GDPR) and aligns with our Information Asset Register.

9.2 If an information asset includes information from different categories, it should be classified as the most sensitive category.

Table 1: The Information Asset Classification System

Security Level	Definition	Examples that SBPR may hold (Not Exhaustive)
Highly Restricted	The information is of significant value. The information is defined under the Data Protection Act 1998 (DPA) as "Sensitive Data". The information is defined under the GDPR as "Special Category Data". Access to the information is restricted to only those who "need to know". Unauthorised disclosure or dissemination could result in: • Severe financial damage, including fines of up to €20m or 4% of our global annual turnover of the previous financial year. • Severe reputational damage. • The revocation of contracts with third parties and the failure to win future contracts / research bids. If this classification of data is held on mobile devices such as laptops, tablets or phones, or in transit, the file / folder must be password protected and the device should have encryption turned on (AES 256-bit encryption at the device, drive or file level). Must be disposed of by shredding.	1. DPA "Sensitive Data" & GDPR "Special Category Data" include data relating to a living individual's (SBPR does not currently collect these data but may in the future consider exploring the diversity and characteristics of its membership): • Race or ethnic origin. • Physical or mental health or condition. • Sexual life or sexual orientation. 2. Salary information. 3. Bank details of an individual. 4. Draft and final reports of a financially / controversially sensitive nature. 5. Passwords. 6. Large aggregates of personal data (e.g. held on membership databases).

Restricted	The information is of especial value. Access to the information is restricted to a small group of staff. Unauthorised access to the information is prevented by password / login. The information is defined under the Data Protection Act 1998 as "Personal Data". The information is defined under the GDPR as "Personal Data". Disclosure or dissemination of this information is not intended, and may incur some negative publicity, but is unlikely to cause severe financial or reputational damage to the SBPR. If this classification of data is held on mobile devices such as laptops, tablets or phones, or in transit, the file / folder must be password protected and the device must be password protected and the device should have encryption turned on (AES 256-bit encryption at the device, drive or file level). Must be disposed of by shredding.	1. DPA & GDPR "Personal Data" include data relating to a living individual's: • Name. • Identification number. • Address. • Phone number. • Email address. • Photographs. • Other personal identifiers such as locations data or online identifier. 2. Confidential meeting minutes. 3. Draft reports or meeting minutes. 4. Draft policy, regulation or course documents.
Internal Use	The information can be disclosed or disseminated to members of the SBPR, including SBPR partners, as appropriate by information owners without any restrictions on content or time of publication. Must be disposed of by confidential waste.	1. Internal correspondence (that is not relating to Restricted or Highly Restricted matters). 2. Final reports / meeting minutes 3. Committee papers. 4. Final policy and procedure documents. 5. Presentation materials owned by others
Public	The information can be disclosed or disseminated to the public without any restrictions on content or time of publication. Disclosure or dissemination of the information must not violate any relevant laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system. May be disposed of by normal waste / recycling.	1. Annual Reports & Financial Statements. 2. Course information. 3. Publicity information. 4. Information published on the SBPR website.

DATA BACKUP

9.3 To minimise the risk of losing data in the event of a systems failure the SBPR Executive Assistant regularly backs up data via Icloud.

9.4 Members of the Executive should also ensure that SBPR related information is backed up securely.

APPENDIX A: SBPR INFORMATION SECURITY CHECKLIST

Key Point	✓
I ensure that I use the Bcc function to send emails to multiple people if their consent has not been obtained for their email address to be shared with others or shared other than for the purpose described in the SBPR's Privacy Notices, i.e. to individuals with an external or personal email address.	
I keep my passwords secure.	
I change my passwords on a regular basis and they are a combination of numbers, letters and symbols.	
I never share my passwords or write them down on paper.	
I ensure that when my computer is not in use, it is electronically locked.	
I understand that leaving my computer open and unattended is presenting itself for a potential data breach to occur.	
I log off from my computer at the end of my working day.	
I shred any personal data that is no longer in use.	
I am vigilant when opening emails from unknown senders or visiting unknown websites, as not doing this can cause the introduction of viruses and other potential harmful malware into the SBPR.	
I will not send, forward or otherwise distribute spam or chain letters.	
I understand that I may only use cloud based storage providers that have been endorsed by the SBPR as to do so otherwise presents a real risk to information security since there is no way the confidentiality, integrity and availability of the information can be assured.	
If I discover a potential, suspected or confirmed information security data breach I will report it immediately to the Data Protection Officer and the Secretary of the SBPR (**contact@sbpr.info**).	

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at www.ncsc.gov.uk/charity .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.
- **Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked, remotely wiped** or **remotely locked.**
- Keep your **devices** (and all **installed apps**) **up to date**, using the **'automatically update'** option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs.**
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges.** This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar,** or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *password*).
- Do not enforce regular password changes; they only need to be changed when you suspect a compromise.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

APPENDIX A: THIRD PARTY SERVICES PROVIDED OR ENDORSED BY THE SBPR

Third Party Service	Acceptable Use of Service	Adequacy Check
UKSSB	For processing of data – sending of emails to members and interested parties with respect to activities of the Society	GDPR compliant
Local conference organiser	Local arrangements associated with society meetings	Awareness of SBPR policy