British Sleep Society
UK Multidisciplinary Sleep Professionals

British Sleep Society (BSS)

Information Security Policy

Related information:

[Information Commissioners Office]

[PCI compliance guide]

[Privacy Policy]

[Data Retention Policy]

[Data Protection Third Party Agreement]

Data Protection Officer: datacompliance@sleepsociety.org.uk

Policy revision:	ISP V1
Issue Date:	June 2019
Next review date:	June 2020

1.0 Policy statement

The purpose of this policy is to set out the British Sleep Society (BSS) aims and objectives for the management of information security throughout the organisation. Information Security is defined as the preservation of confidentiality, integrity and availability of information.

This policy is intended to establish the necessary procedures and an organisational structure that will protect the British Sleep Society (BSS), its information assets and critical activities from all appropriate threats and to ensure regulatory, statutory, contractual and legislative requirements are met.

Compliance with this policy is necessary to ensure business continuity, and to minimise the impact of any security incidents that may occur and so reduce the potential damage to the BSS and its membership.

2.0 Scope

The scope of the data protection policies cover the storage, access, transmission and destruction of information.

The policy is aimed at those authorised to conduct business on behalf of The BSS including Committee and subcommittee members, Data Processors and others with access to information (wherever the information is located) as well as the applications, systems, equipment and premises that create, process, transmit, host, or store information, whether in-house, personally owned or provided by external suppliers.

3.0 Definitions and Terms

- **Confidential data** includes, but is not limited to, information for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the BSS if disclosed or modified e.g. credit card details.
- **Internal Use data** includes, but is not limited to, information that BSS considers should be protected to prevent unauthorised disclosure by a third party
- **Public data** is information that may be freely disseminated.
- **Media** is defined as emails, any printed or handwritten paper, received faxes, USB devices, back-up tapes, computer hard drive, etc.
- **PCI DSS** is the worldwide Payment Card Industry Data Security Standard that help businesses process card payments securely and reduce card fraud. Achieved through enforcing tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data.

4.0 Information security principles

The following information security principles provide overarching governance for the security and management of confidential information and personal data.

- Confidential information and personal data should be both secure and limited to what is necessary to complete a task.
- Confidential information and personal data will be protected against unauthorised access and processing.
- Breaches of this policy must be reported to the Data Protection Officer.

4.1 Information Security

BSS and its Data Processors regularly handle information including member, delegate and cardholder data. Such information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

The BSS commits to respecting the privacy of all individuals it holds and processes data on, including its members, delegates and committee members and to protecting any data it holds from outside parties.

Any individual including but not limited to Committee Members and Data Processors handling data on behalf of BSS should ensure that:

- Personal data and cardholder information is handled in a manner that fits with its sensitivity.
- E-mail, internet and other resources are not used to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
- Unless previously defined, personal or sensitive information is not disclosed unless authorised by the Data Protection Officer. If it is unclear whether data is personal/ sensitive or not, the Data Protection Officer will be contacted to clarify.
- Sensitive data such as cardholder information is protected by only using Data Processors that have been screened and approved for using current legalisation such as PCI DSS compliance.
- Passwords and accounts are kept secure.
- Accidental access to personal data is reduced by keeping work areas clear of personal data and computer screens are locked when unattended.
- Information security incidents are reported, without delay, to the Data Protection Officer.

The BSS reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose. All individuals who conduct business or who process or store data on behalf of the BSS have responsibility for ensuring that systems and data are protected from unauthorised access and improper use.

If you are unclear about any of the policies detailed herein, you should seek advice and guidance from the Data Protection Officer.

4.3 Cloud based service providers

BSS and its Data Processors use cloud based service providers to be able to carry out BSS activities. BSS retains responsibility as the data controller for any data it puts into the service, and can consequently be fined for any data breach, even if this is the fault of the Cloud service provider. It is the responsibility of any Data Processor to inform BSS of any breach. BSS will also bear the responsibility for contacting Information Commissioner's Office concerning the breach, as well as any affected individual. It will also be exposed to any lawsuits for damages as a result of the breach. It is extremely important, as a consequence, that BSS is able to judge the appropriateness of a Cloud service provider's information security provision.

This leads to the following stipulations:

- Cloud service companies must be PCI certified providers if the service is card payments
- Cloud services used to process personal data will be expected to meet the GDPR principle of privacy by design, and that it has considered information security throughout its service model
- Any individual wishing to use non approved service providers for BSS activities must request permission from the Data Protection Officer

Please see Appendix A for a list of current service providers.

4.4 Protecting stored data

- Technologies should be used and setup in acceptable network locations
- Keep passwords secure and do not share accounts
- Authorised users are responsible for the security of their passwords and accounts
- All electronic devices used to process sensitive data must have password protected access
- Because information contained on portable devices is especially vulnerable, special care should be exercised

All personal and sensitive data stored and handled by the BSS and its Data Processors must be securely protected against unauthorised use at all times. Any data that is no longer required by the BSS for organisational reasons must be disposed of in a secure and irrecoverable manner. Please find more information regarding the storage and deletion of data on the BSS Data Retention & Destruction Policy.

4.5 Access to data

All access to data should be controlled and authorised. Any job functions that require access to data should be clearly defined.

Access to information such as personal and organisation data is restricted to those that have a legitimate need to view such information.

4.6 Third party access to data

- All third-party companies providing critical services to the BSS must provide a signed Service Level Agreement or Third Party Agreement. Please refer to the Data Protection Third Party Agreement link under 'Related Information' on the first page.
- All third-party companies which have access to information must:
    - Adhere to the PCI DSS security requirements for cardholder data if applicable
    - Acknowledge their responsibility for securing the data
    - Acknowledge that cardholder data must only be used for assisting the completion of a transaction, providing a fraud control service or for uses specifically required by law.
    - Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
    - Be compliant with current Data Protection legislation, whether based in or outside of the European Union.

Please see Appendix A for a list of current service providers.

4.7 Protecting data in transit

All personal and sensitive data must be protected securely if it is to be transported physically or electronically.

- Portable devices storing or transferring personal data should be password protected and such passwords should be kept securely and not shared.
- When transferring personal data via email, such as delegate or member spreadsheets, such files should be password protected with the password being sent on a separate email.

5.0 Forms

Agreement to Comply Form - Appendix B

Appendix A

List of Service Providers

Name of Service Provider	Services Provided	PCI DSS Compliant	GDPR Compliant
Executive Business Support Ltd	Administration, accounting and event organisation	Yes	Yes https://execbs.com/privacy-policy/
Wheeler & Co Ltd	Accountants	n/a	Yes

List of Cloud based Service Providers

Name of Service Provider	Services Provided	PCI DSS Compliant	GDPR Compliant
Events Air	Event administration	Yes https://eventsair.com/blog/gdpr-and-the-event-professional/	Yes https://eventsair.com/privacy-policy/
Mailchimp	Email communication	n/a	Yes https://mailchimp.com/legal/privacy/
Stripe	Card payments - events	Yes https://stripe.com/guides/pci-compliance#how-stripe-helps-organizations-achieve-and-maintain-pci-compliance	Yes https://stripe.com/gb/privacy
WP Engine	Website hosting	Yes/self-certify https://wpengine.co.uk/support/wp-engine-and-pci-compliance/	Yes https://wpengine.com/legal/privacy/
Fast2host	Website Host and e-mail exchange	Yes	Yes https://www.fast2host.com/legal/privacy-policy

Appendix B

Agreement to comply form – agreement by Committee members, Sub-committee members and all those who process personal data on behalf of the British Sleep Society (BSS), to comply with information security policies

_____

Name (printed)

_____

Date

I agree to take all reasonable precautions to ensure that BSS internal information, or information that has been entrusted to BSS by third parties such as members and delegates, will not be disclosed to unauthorised persons. At the end of my tenure with BSS, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use personal or sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of BSS.

I have access to a copy of the Information Security and Data Protection policies and I have read and understand these policies. As a condition of continued tenure, I agree to abide by the policies. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the Data Protection Officer.

_____

Signature