

The British Sleep Society (BSS)
***Data retention and
destruction policy***

Related information:

[BSS Privacy Policy](#)

[Information Commissioners Office](#)

Policy revision:

DRP V1

Issue Date:

May 2019

Next review date:

May 2020

Contact for document:

datacompliance@sleepsociety.org.uk

1.0 Policy statement

This policy represents the practice of the British Sleep Society (BSS) with respect to the retention and destruction of documents and other records, both in hard copy and electronic media (which may be referred to as “documents” in this policy) that contain personal and/or sensitive information. The purposes of the policy include (a) storage and maintenance of documents necessary for the proper functioning of the organisation as well as to comply with current legal requirements; and (b) the destruction of documents which no longer need to be retained. BSS is required by current Data Protection law, to securely dispose of data when it is no longer required regardless of the media or application type on which it is stored.

BSS reserves the right to revise or this policy at any time.

2.0 Scope

This policy is relevant to the Executive Committee, members of relevant sub-committees, Data Processors and any individual who process personal data on behalf of BSS.

3.0 Definitions

Documents – refers to any item containing data whether in hard copy or in any electronic format

Personal data – data which can be used to identify an individual

4.0 Procedures

In order to comply with this policy, the processes in this section **must** be adhered to.

More information regarding relevant timeframes can be found in detail in Appendix 1.

4.1 Hard copy document storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it or see it. Guidelines below regarding data held on paper files should be followed:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Paper and printouts are not left where unauthorised people could see them e.g. on a printer or scanner etc.
- Hard copy financial documents containing details such as a person’s bank details, must be locked away securely.
- End of year financial records need to be filed appropriately and held securely in a locked cupboard until transferred to an approved storage facility.

4.2 Hard copy document destruction

- Printouts with personal data should be kept securely whilst in use and disposed of securely when no longer required. Refer to destruction requirements below and Appendix 1 for more information.

- The destruction of hardcopy (paper) materials must be crosscut shredded, incinerated or pulped so they cannot be reconstructed. Until this time, these must be kept locked away and clearly marked “To Be Shredded” - access to these files must be restricted.

4.3 Electronic document storage

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and hacking attempts. The following requirements are listed for this purpose but are not exhaustive; it is an individual’s responsibility to ensure they are working to these requirements:

- Personal and financial data held on databases and spreadsheets should be protected by strong passwords that are changed regularly and never shared.
- If data is stored on portable devices (like a USB, laptop, CD or DVD), these should be kept locked away securely and then securely wiped when no longer required.
- Data should only be uploaded to approved cloud computing services that has individual password access.
- Access to servers containing personal data should be secure and the server itself must be stored in a secure location.
- Data should be held in as few places as necessary. Duplicate records or data sets should be deleted unless the reason for their duplication is for BSS continuity back-ups.
- Data stored should have suitable backups to protect against data failure, corruption or outside interference.

4.4 Electronic document destruction

- Confidential and sensitive electronic data must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media. If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion. Please follow your institutions destruction process if applicable.

4.5 Emergency document storage

Documents which are necessary for the continued operation of BSS, in the case of a significant business disruption, shall be stored in a safe and accessible manner. Electronic documents will be regularly duplicated or backed up.

4.6 Archive storage

BSS retains documents and information in both electronic and hard copy archives. Only necessary documentation should be retained.

4.7 Third party storage providers

Only third party storage providers that have been researched and match BSS security standards should be used. Please see the approved list of third party providers for more information. If you are unsure, please contact the BSS Data Protection Officer.

All third party storage providers should be monitored and any unwanted documents and information should be removed.

5.0 Responsibilities

The Executive Committee, Data Protection Officer and Data Processors are responsible for implementing this policy and ensuring regular reviews and updates are made.

APPENDIX 1: Data retention and disposal schedule

Data item(s)	Description	Retention period
BSS General Documents	<ul style="list-style-type: none"> Articles of Association 	Life of organisation
	<ul style="list-style-type: none"> AGM Meeting minutes 	Life of organisation
	<ul style="list-style-type: none"> Committee papers 	Life of organisation
	<ul style="list-style-type: none"> Committee agendas 	Life of organisation
	<ul style="list-style-type: none"> Informal minutes and action logs 	6 years
	<ul style="list-style-type: none"> Policies 	Scheduled reviews and ongoing updates, previous versions 6 years
Financial management: (Bank, petty cash and creditors records)	<ul style="list-style-type: none"> Paid/presented cheques and records of all cheques drawn for payment 	7 years
	<ul style="list-style-type: none"> All other cheque records – cheque books received, butts, cancelled cheques etc. 	7 years
	<ul style="list-style-type: none"> Bank statements and reconciliations 	7 years
	<ul style="list-style-type: none"> Electronic banking – transactions, payment files, deposits, withdrawals and audit trail 	7 years
	<ul style="list-style-type: none"> Creditors history records, lists and reports 	7 years
	<ul style="list-style-type: none"> Statements of accounts 	7 years
Financial management: Ledger records	<ul style="list-style-type: none"> General ledger produced for purposes of preparing certified financial statements 	7 years
	<ul style="list-style-type: none"> Creditor ledger 	7 years

	<ul style="list-style-type: none"> • Other ledgers and related audit trails 	7 years
	<ul style="list-style-type: none"> • Customer invoices 	7 years
	<ul style="list-style-type: none"> • Supplier invoices 	7 years
	<ul style="list-style-type: none"> • Supplier statements 	7 years
	<ul style="list-style-type: none"> • Annual and quarterly financial statements 	7 years
Financial customer purchase records	<ul style="list-style-type: none"> • Purchase order records 	7 years
	<ul style="list-style-type: none"> • Details of membership receipts 	7 years
	<ul style="list-style-type: none"> • Events registration receipts 	7 years
Financial management: income and expenditure	<ul style="list-style-type: none"> • Debtors/creditors records and invoices 	7 years
	<ul style="list-style-type: none"> • Credit notes and refunds 	7 years
	<ul style="list-style-type: none"> • VAT Returns 	7 years
	<ul style="list-style-type: none"> • Companies House submissions 	7 years
	<ul style="list-style-type: none"> • Charities Commission submissions 	7 years
Committee members	<ul style="list-style-type: none"> • Contact details including address 	6 years following cessation of tenure
	<ul style="list-style-type: none"> • Declaration of Interest 	6 years following cessation of tenure
	<ul style="list-style-type: none"> • Expense claims and authorisation 	7 years
	<ul style="list-style-type: none"> • Biographies and photographs 	Review 2 years following cessation of tenure

Events	<ul style="list-style-type: none"> • Delegate registration forms 	3 years after event
	<ul style="list-style-type: none"> • Attendance signatures 	5 years
	<ul style="list-style-type: none"> • Photographs 	Reviewed after 5 years
	<ul style="list-style-type: none"> • Supplier contracts and payments 	7 years
	<ul style="list-style-type: none"> • Speaker presentations 	3 years after event
	<ul style="list-style-type: none"> • Speaker details (contact, biographies and photographs) 	3 years after event
	<ul style="list-style-type: none"> • Exhibition and sponsorship company information including sponsorship payments and contact details 	7 years
	<ul style="list-style-type: none"> • Company logo and profiles 	6 months after event
	<ul style="list-style-type: none"> • Abstracts 	3 years after event
	<ul style="list-style-type: none"> • Bursary applications 	7 years
	<ul style="list-style-type: none"> • Award/ prize winners details inc. name and photograph 	Reviewed after 10 years
	<ul style="list-style-type: none"> • Rooming requirements 	Financial records for 7 years, general details delete after event ends
Training and Examination Documents	<ul style="list-style-type: none"> • Final marks and results 	Life of the organisation
	<ul style="list-style-type: none"> • Working documents 	1 year following completion of exam or training
	<ul style="list-style-type: none"> • Additional personal details separate to Final Marks and results identification 	1 year following completion of exam or training
Members	<ul style="list-style-type: none"> • Applications 	1 year

	<ul style="list-style-type: none"> • Contact details 	6 years after membership ends
	<ul style="list-style-type: none"> • CV and qualifications 	1 year after membership ends
	<ul style="list-style-type: none"> • Membership and payment history 	7 years
Other	<ul style="list-style-type: none"> • Email addresses on general mailing list 	6 years