British Toxicology Society
Data retention and destruction policy

Related information:

BTS Privacy Policy
Information Commissioners Office

Policy revision:	DRP V1
Issue Date:	September 2018
Next review date:	September 2019
Contact for document:	secretariat@thebts.org

Data retention and destruction policy

1.0 Policy statement

This policy represents the practice of The British Toxicology Society (BTS) with respect to the retention and destruction of documents and other records, both in hard copy and electronic media (which may merely be referred to as "documents" in this policy). 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. BTS is required by law, to securely dispose of data when it is no longer required regardless of the media or application type on which it is stored.

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

2.0 Scope

This policy is relevant to elected officers, members of the Executive Committee, members of relevant sub-committees and Data Processors.

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 in the cupboards provided.
- End of year financial records need to be boxed up and held securely in a locked cupboard until transferred to storage.

4.2 Hard copy document destruction

- Printouts with personal data should be shredded and disposed of securely when no longer required. Refer to Appendix 1 for more information.

- Hard copy bank statements should be retained for the legal requirement of 7 years and then disposed of confidentially.

- 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

- Personal and financial data held on databases and spreadsheets should be protected by strong passwords that are changed regularly and never shared between employees.

- 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.

- 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 BTS continuity back-ups.

- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and hacking attempts.

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 BTS, in the case of a significant business disruption, shall be stored in a safe and accessible manner. These documents will be regularly duplicated or backed up. Please follow your institutions back-up process if applicable.

4.6 Archive storage

BTS 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 BTS security standards should be used. If you are unsure, please contact the BTS Data Protection Officer. Such third party providers include, but are not limited to:

- Dropbox
- Events Air
- SAGE

These should be monitored and old and unwanted documents and information from such third party sites should be removed.

5.0 Responsibilities

The President, 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
BTS General Documents	• Memorandum of Association	Life of organisation
	• AGM Meeting minutes	Life of organisation
	• Committee papers	Life of organisation
	• Committee agendas	Life of organisation
	• Informal minutes and action logs	6 years
	• Policies	Scheduled reviews and ongoing updates
Financial management: (Bank, petty cash and creditors records)	• Paid/presented cheques and records of all cheques drawn for payment	7 years
	• All other cheque records – cheque books received, butts, cancelled cheques etc.	7 years
	• Bank statements and reconciliations	7 years
	• Electronic banking – transactions, payment files, deposits, withdrawals and audit trail	7 years
	• Creditors history records, lists and reports	7 years
	• Statements of accounts	7 years
Financial management: Ledger records	• General ledger produced for purposes of preparing certified financial statements	7 years
	• Creditor ledger	7 years

	• Other ledgers and related audit trails	7 years
	• Customer invoices	7 years
	• Supplier invoices	7 years
	• Supplier statements	7 years
	• Annual and quarterly financial statements	7 years
Financial customer purchase records	• Purchase order records	7 years
	• Details of membership receipts	7 years
	• Events registration receipts	7 years
Financial management: income and expenditure	• Debtors/creditors records and invoices	7 years
	• Credit notes and refunds	7 years
	• VAT Returns	7 years
	• Companies House submissions	7 years
	• Charities Commission submissions	7 years
Committee members	• Contact details including address	6 years following cessation of tenure
	• Declaration of Interest	6 years following cessation of tenure

	• Expense claims and authorisation	7 years
	• Biographies and photographs	Review 2 years following cessation of tenure
Events	• Delegate registration forms	3 years after event
	• Attendance signatures	5 years
	• Photographs	Reviewed after 5 years
	• Supplier contracts and payments	7 years
	• Speaker presentations	1 year
	• Speaker details (contact, biographies and photographs)	1 year
	• Exhibition and sponsorship company information including sponsorship payments and contact details	7 years
	• Company logo and profiles	6 months after event
	• Abstracts	3 years after event
	• Bursary applications	1 year
	• Award/ prize winners details inc. name and photograph	Reviewed after 10 years
	• Rooming requirements	Financial records for 7 years, general details delete after event ends
Members	• Applications including referee details	1 year

	• Contact details	6 years after membership ends
	• CV and qualifications	1 year after membership ends
	• Membership and payment history	7 years
Other	• Email addresses on general mailing list	6 years