Dorset and Bournemouth, Christchurch & Poole Safeguarding Adults Boards

Document Retention Policy and Destruction Schedule

Strategy approved	26 June 2023	Review Date	June 2026

1. Introduction

Dorset and Bournemouth, Christchurch & Poole Safeguarding Adults Boards (DBCPSABs) are committed to complying with the law and regulations in all our business activities, including applicable Data Protection Legislation and to using all appropriate technical and organisational measures to ensure the protection of any personal data collected, whilst undertaking statutory duties.

This policy explains how the Boards shall retain and dispose of data and provides guidance on appropriate data handling and disposal schedules.

Failure to comply with this policy may expose the Boards to fines and penalties, adverse publicity, and difficulties in providing evidence when it is needed as well as undertaking statutory duties. Any references to "DBCPSAB", 'we,' 'our' and 'us' refer to the Dorset and Bournemouth, Christchurch & Poole Safeguarding Adults Boards.

It is recognised that all partner agencies will have their own data handling and destruction policies which they will need to follow.

2. Scope

This policy covers all data that DBCPSAB holds or has control over. This includes physical data such as hard copy documents, contracts, and letters. It also includes electronic data such as emails, electronic documents, and audio recordings.

There may be legal and regulatory requirements for us to retain data for a specified period of time. However, we also retain data to help us operate and to have information available when we need it. Retaining data for longer than necessary can expose us to risk as well as be an additional cost. It is therefore essential that we record and maintain a register of the data we hold, including where it is held and who has access to it, in a systematic and reliable way.

A vital part of the DBCPSAB Document Retention Policy and practice is that personal data is retained for the appropriate period of time and kept for no longer than is necessary. It is paramount that the retention period allows the Board to meet its legal and regulatory requirements but that the rights of data subjects are also protected.

This policy has been developed to help the DBCPSABs to effectively manage data in a consistent manner. This policy is also supported by the Retention and Destruction Schedule which defines what data is held and how long we shall retain the data for / when the data will be disposed of. (Appendix 1)

3. Guiding principles

Through this policy, and data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to comply with out statutory obligations effectively, but we do not create or retain data without good reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.

- We regularly monitor and audit compliance with this policy and update this policy when required.

Roles and Responsibilities

All DBCPSABs staff, including those with whom we contract to author Safeguarding Adult Reviews and third parties who process data on our behalf, are responsible for complying with the requirements of this policy. The DBCPSAB Business Managers are responsible for maintaining the policy and monitoring compliance.

4.Storage and Back-up

Data must be stored in a safe, secure, and accessible manner. All documents must be backed up at least daily.

5. Retention Periods

Please see attached Retention and Destruction Schedule (Appendix 1)

Hard copy and electronically held records, documents and information must be deleted or securely destroyed at the end of the retention period.

6. Suspending the destruction date in special circumstances

If a claim, audit, investigation, subpoena, or litigation has been asserted, or filed by or against us, or is reasonably foreseeable, we have an obligation to retain all relevant records, including those that otherwise would be scheduled for destruction under our Retention and Destruction Schedule. Equally records will be kept if the subject of a Safeguarding Adult Review is also subject to a Coroner's Inquest at a future date.

A record will be kept of any decision to retain information in excess of the usual retention period and the necessity to continue to retain the information will be reviewed at least annually.

7. Methods of Destruction

All data, whether hard copy or electronic must be destroyed in a secure manner, preserving the confidentiality of all personal data.

All hard copy data must be disposed of in confidential waste bins or shredded. Under no circumstances should confidential or personal data be put into normal waste bins, unless shredded.

Electronic data will be securely destroyed in a way which cannot be recovered. The DBCPSABs Business Team, including those with whom we contract to author Safeguarding Adult Reviews, will also be responsible for ensuring that any electronic data is securely wiped from email and personal storage when the central records are destroyed. It is therefore important that The DBCPSABs Business Managers maintain contact with independent SAR authors to ensure that any documents held by the SAR authors are also disposed of at the same time.

The DBCPSABs Business Managers are responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction.

8. Breach and Incident Reporting

8a. The effectiveness of delivering against this policy is dependent upon the Boards Business Team, the Independent Chair and authors of Safeguarding Adult Reviews. All other Board partners operate in the context of their own organisational data protection policy. If it is known that someone may have breached the Board policy, the matter will be reported immediately to the DBCPSABs Business Team and to the appropriate Board partner organisation.

8b. Breach or Incident

Data Breach means personal or confidential information that has been seen by someone who should not see it.

An **Incident** means personal or confidential information has been put at risk of someone seeing it, but this has been prevented. See Appendix 2 for examples of breaches.

8c. Breach/Incident Reporting

You will receive a reporting form from Information Governance or your organisations equivalent. The officer responsible for the breach will need to complete part of the form and then pass it to their manager. An investigation will need to take place, all relevant people will need to be contacted and remedial action considered. The process will follow that agreed by your organisation.

9. Audit

An annual audit will be carried out to assess compliance with this policy including ensuring that data is being retained and disposed of in adherence with the Retention and Destruction Schedule.

10. Review

This policy is owned by the DBCPSABs and will be reviewed at least annually by the DBCPSABs Business Managers.

The DBCPSABs Business Managers will ensure that any changes to this Policy are circulated, and training provided (where appropriate).

Appendix 1 Retention of Dorset and BCP SAB Documents

Safeguarding Adult Reviews (SARs)	All documentation relating to SARs & SAR referral information such as Chronologies and Information Management Reviews (IMRs); Reports from partner agencies as well as SAR author information; notes of meetings or events, Email Records, SAR Terms of Reference; Medical Information and Family details	Content of file to be deleted 3 years after publication of the review with the exception of the following and after conclusion of any future legal process e.g., Coroner's Inquest: • Original and PDF versions of the report • Original and PDF versions of executive summary • Original and PDF version of 7 Minute Learning briefings The three items listed above will be retained for a period of 10 years after publication.
Non-Statutory Reviews	All documentation relating to the review: Referral information, Chronolator and IMRs, Author information, Meetings and Events, Email Records, Terms of Reference, Panel Membership, Medical Information, Family details	Content of all notes in preparation of the review to be deleted 3 years after publication of the review with the exception of the following and after conclusion of any future legal process e.g., Coroner's Inquest: • Original and PDF versions of the report • Original and PDF versions of executive summary • Original and PDF version of Learning briefings The three items listed above will be retained for a period of 10 years after publication.
Meetings	All documentation relating to personal data shared at DBCPSAB meetings	All records to be deleted 5 years subsequent to the date of the meeting, with the exception of Terms of Reference which will be deleted 2 years after publication of an updated version.
Consultancy contracts	Consultancy contracts created for: SAR Authors Chair of the Board Deputy Chair of the Board	Content of file to be deleted 3 years after end of contract
Policy and Procedures	Copies of Board policies, procedures, protocols, flowcharts and templates.	All copies and supporting documentation of policies, procedures, protocols, flowcharts or templates are to be deleted 5 years after publication of superseding versions.
Audits	Information collected as part of an audit. Collated data created as part an audit.	All records, collected information and collated data to be deleted 2 years after audit is completed
Board Emails	Requests for general support/advice	To be kept for keep for 12 months.

Appendix 2 Examples of Breaches

For example: An email sent to the wrong person, which is then opened and read, is a breach. An email sent to the wrong person, which is deleted before being read, is an incident. It is important to record both incidents and breaches because information has been at risk, it is only the outcome which is different.

Types of common breaches

• Sending emails to the wrong person

• Leaving confidential information at the printer • Sending information to the wrong address/wrong person

• Disclosing information without a lawful reason to • Leaving information on view

• Losing case files, diaries, minutes, notebooks

• Losing equipment/stolen equipment

• Accessing computer records about family/friends/neighbours