Sightsavers

Data Retention Policy

Sightsavers

Sightsavers

Document control

Policy Owner	**Sightsavers Management Team**
Policy Administrator	**Controller of Governance and Assurance**
Document Status	**Draft**
Version Number	**1.0**
Review period	**3 years**

Document amendment history

Version number	Date	Amendment summary	Approved by
1.0	May 2026	First Published in new format	

Contents

1. Definitions

Data and/or records	All information, whether held electronically or in paper format, not limited to those containing personal data (such as a name, address and contact details), including any financial documentation, company records, employee information, photographic images, video content, audit accounts, medical records, donor information, survey results, research data and any other data and records stored by Sightsavers .
Data Retention Schedules	The retention periods in respect of categories of documents agreed by the Information Owners and as prescribed by laws such as UK GDPR, Freedom of Information Act, Limitation Acts, Finance Acts and the Companies Act. In jurisdictions outside the UK, retention principles and periods are prescribed by laws such as the NDPR (Nigerian Data Protection Regulation), or the Data Protection Act in Kenya, in addition to other laws relating to limitation periods, and they may be referenced in the relevant schedules.
Information Owner	Directorates review relevant sections of the Data Retention Schedules and are responsible for deciding how long to keep data and records and for implementing their storage and disposal.
Sensitive data	Data that is confidential or personal in nature, or which falls within the GDPR definition of “special category data” including, but not limited to, data relating to the health, ethnicity and religion status of living individuals.

2. Introduction

2.1 Policy Objective and Overview

This policy sets out the principles for ensuring that Sightsavers implements effective and compliant data and records management. Together, the Retention Policy and the Retention Schedules provide essential guidance to staff to help them meet their obligations in respect of retention, storage and disposal of records and data.

Some laws require certain records to be kept for a specific period (for example, many financial records must be kept for at least 6 years in addition to the current financial year in accordance with tax law). At the same time, data protection and privacy laws, and our Data Protection Policy, require that we do not keep personal data for longer than necessary and that we minimise the personal data that we do retain.

It is also crucial that we do not retain personal data for longer than necessary to reduce information security risks to Sightsavers and to minimise risks to the people whose personal information we store. We must also meet contractual commitments and those that we have

given to our beneficiaries, supporters and employees, when collecting their personal data. Disposal of records and data can also provide financial and environmental efficiencies.

2.2 Policy Scope

This policy applies to all Sightsavers staff and all other parties with access to Sightsavers' information or IT systems.

Sightsavers' Retention Schedules set out the time periods that different types of records and data must be retained for legal and business purposes, however, the decision as to how long to retain data is ultimately made by the Information Owner.

Data owned by Sightsavers, but held and/or processed by third parties must also be retained according to the Retention Schedule(s). All suppliers that process personal data on behalf of Sightsavers (eg. supporter data and beneficiary data) must have a data processing agreement in place with Sightsavers, which is compliant with the relevant regulation. This agreement should set out the data retention commitments of the supplier. The Information Owners are responsible for monitoring and reviewing these suppliers to ensure that these commitments are met.

2.3 Other relevant policies

This policy should be read and understood in conjunction with Sightsavers' Data Protection Policy, IT Security Policy, IT Usage Policy, Social Media Policy, Supporter Promise and Privacy Statement, Employee Data Privacy Notice and any other relevant guidelines or policies.

3. Retention and Storage

3.1 Retention Responsibilities

Information Owners should devise their own processes for assessing their records management and should prepare a register of records and information. All members of staff are responsible for securely storing and destroying records in line with the appropriate Retention Schedule and the Information Owner's agreed process.

3.2 Retention Justification

There must be an appropriate justification for retaining data and records (operational, business, contractual or legal reasons) and the justification needs to be proportionate in the circumstances. For example, it is easier to provide a justification for retaining data that contains no personal data and has little commercial sensitivity, than to justify retaining health data of identifiable beneficiaries without taking into account a range of issues such as the law relating to this data, the consent (if that was the legal basis for processing the data – see the Data Protection Policy) and the purposes of the data processing.

In the UK and EU, the General Data Protection Regulation (GDPR) and UK GDPR requires that records containing information on identifiable living individuals should not be kept for

longer than is necessary for the purposes for which it was obtained and processed (there are some exceptions where data is processed for archiving, scientific, research or statistical purposes). Other jurisdictions may have similar regulations in force, and we should apply the same principle wherever we work.

3.3 Retention Decision

When faced with a decision about a document, or a set of documents, Information Owners should consider the following questions:

- Has the information come to the end of its useful life?
- Is there a legal requirement to keep this information or document for a set period? (Refer to the relevant Retention Schedule).
- Could the information be required in the case of any legal proceedings? (Is the information contentious, does it relate to an incident that could potentially give rise to proceedings?) Is there any active access request to this information from a data subject (eg. employee, supporter, beneficiary)?
- Would the document be useful for the organisation as a precedent, learning document, or for performance management processes? In determining this, risks of holding the information should also be taken into account; a 'just because it might be useful' approach, will not be a valid reason.

3.4 Storage

Sightsavers' Information Security Policy must be followed when storing digital data and records.

The Information Owner is responsible for ensuring that the records are stored in a safe, secure and accessible manner, which includes ensuring that:

- Reasonable controls are in place to ensure the security and accuracy of the records;
- Reasonable controls are in place to prevent the loss of records;
- Records are not removed from or stored outside of Sightsavers' systems or premises;

When storage space for hard-copy records is an issue, in the UK office, Sightsavers uses a contracted offsite storage provider. This can be a cost-effective way of managing records, but careful thought should be given to the types of records that are selected for offsite storage, in particular how quickly and frequently such records may need to be accessed.

Retention can be complicated if records of a dissimilar nature, with different retention requirements, are filed together. Information Owners should consider retention periods when designing their records storage systems and embedding practices to avoid this issue. Files should be weeded regularly to ensure records are not kept for too long. If there is no alternative, the entire file should be retained for the longest relevant retention period.

In some circumstances it may be necessary to retain a record for longer than its defined retention period (see 3.3 above). If a record needs to be retained for longer, then a new retention timescale should be assigned to it. It is recommended that this date should not be too far in the future, enabling regular review of the decision while taking circumstances into account. A period of one year between reviews is recommended.

3.5 Anonymisation & Pseudonymisation

Where there is a good reason to keep records, you may be able to anonymise it to enable this without infringing the data retention principles relating to personal data. For example, you may be required to delete personal data that was collected and stored on the basis of consent which was given for 5 years, but once that data is anonymised, it may be retained for longer periods.

Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. Once data is truly anonymised and individuals are no longer identifiable, the data will not fall within the scope of privacy regulations and it becomes easier to use. There may be good reasons to anonymise certain data, such as for research purposes. Pseudonymisation is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, such as a securely stored register containing the names and corresponding and ID numbers.

Unlike anonymisation, pseudonymisation of data does not take the information out of many privacy regulation obligations, but it reduces risks to the individual and supports the principle of data minimization, and it therefore may be considered as part of a range of approaches towards good privacy practices set out in the Data Protection Policy.

4. Disposal of Data

Implementing the disposal of data can be a challenging task. Information Owners are responsible for ensuring that those responsible for processing the data are implementing disposal of the data once the relevant retention period has expired.

4.1 Destruction of Records

The following disposal principles should be followed:

- Disposal methods used must be appropriate to the level of sensitivity or confidentiality of the records in question. The destruction of confidential, financial and personnel-related records must be conducted by shredding or secure electronic deletion as appropriate.
- All copies, duplicates and back-ups of records must be disposed of at the same time as the original record, unless there is a valid legal or business reason not to; and
- An appropriate record must be made of the record disposals.

www.sightsavers.org
Registered charity numbers 207544 and SC038110

Sightsavers