Guidance on Records Retention

This document is designed to be read in conjunction with the **Authority's Data Protection Policy** and **the Information Management Framework Policy** and sets out guidance on the retention and disposal of all records

It is important to remember that retention guidance applies to **all documents defined as records,** not just **personal data**.

In terms of personal information, the General Data Protection Regulation (GDPR) states that personal data 'shall not be kept for longer than is necessary for the purpose of processing'. The basic objective of this principle is that organisations do not retain obsolete data. The Regulation does not offer any guidance on record retention for the purposes of audit, archive, reference etc, instead leaving such decisions to individual organisations.

Annex A Flowchart: Key considerations for retaining or disposing of documents

Annex B Retention of Personal Data gives some suggested points to consider when reviewing discretionary retention periods for personal information.

Annex C: Proposed retention schedule

1. **Aims**

   The purpose of putting in place good records and information management procedures is to ensure that records are kept in such a way that:

   - they can readily be retrieved when required
   - ensures accountability and provides an audit trail
   - allows records to be identified for historical and research purposes
   - protects information which is a valuable resource

2. **Definitions and terminology**

   "**Records'"**" are defined as information created, received and maintained as evidence and information by an organisation or person in pursuance of legal obligations or in the transaction of business

   "Information asset" any piece or collection of information we hold, defined and managed as a single unit so that we can understand it, share and protect it effectively and get the most value from it. It is something we can't replace without cost, time, skill and resources. Information assets have a recognisable and manageable value, risk, content and lifecycles

   "**Retention**" usually means the length of time for which records are to be kept, prior to disposal. Some records, for example committee papers, planning applications and decisions or legal documents, there is a statutory requirement to retain for a specified period/in perpetuity. For other records, the retention period is discretionary and a judgement must be made by the "owner" of that record.

   "**Disposal**" in this context does not just mean destruction: it includes any action taken [or yet to be taken] to determine the fate of records including transfer to a permanent archive.

Where it is not possible to determine the timescale for disposal of the records, they should be scheduled for review at a later date

3. Why do we need a Document Retention Schedule?

The benefits in having a retention schedule are to:

- ensure records are retained only for as long as there is a need
- reduce the volumes and costs of both paper and electronic records storage
- prevent duplicates being maintained
- make it easier to find and share information
- improve the working environment by reducing storage space
- comply with specific legal and regulatory requirements including those under the Freedom of Information Act 2000/Environmental Information Regulations 2004 and the GDPR 2016
- support accountability - including the availability of archived records of genuine historical value.

4. Practical Considerations

Records should be kept for as long as there is a business need or legislation requires. This will vary from between 6 months and in perpetuity. Records relating to HR and Financial activities will have well-defined retention periods. Many organisations that provide grant funding such as HLF will also set out defined periods for retention of particular project/financial documents.

In circumstances where the retention period of a record is unclear, the recommended default is taken to be 6 years.

Each Service is responsible for managing its records and to assist with this and to meet our obligations under the GDPR, we've defined an Information Asset Register which in turn is maintained by a team of Information Asset Owners (IAO). Our IAOs are senior members of staff (generally Heads of Service or Team Managers) who are responsible for ensuring that the information asset is accurately recorded and managed. To help with this we have introduced the Informu asset management system which will provide the following benefits:

- maintain an inventory of information assets
- maintain retention policies and map them to a business classification scheme
- analyse records to inform our record keeping strategy and address information risks
- support the production of information for Records of Processing Activities (ROPA) under GDPR Article 30 compliance
- support ISO27001 (international information security standard) compliance
- record ongoing transactions, such as disposals, to maintain an ongoing audit trail of business events related to the assets
- use workflow to create instructions for business events relating to assets such as notifications and alerts identifying assets due for review/disposal*.

**Records that are identified for archive or disposal – all copies of the records should be identified including those in paper format, filed on the network, located on hard drive and*

USB sticks, web and in Outlook folders. ***NB – check for multiple copies, including all versions***.

5. Outlook storage/email accounts

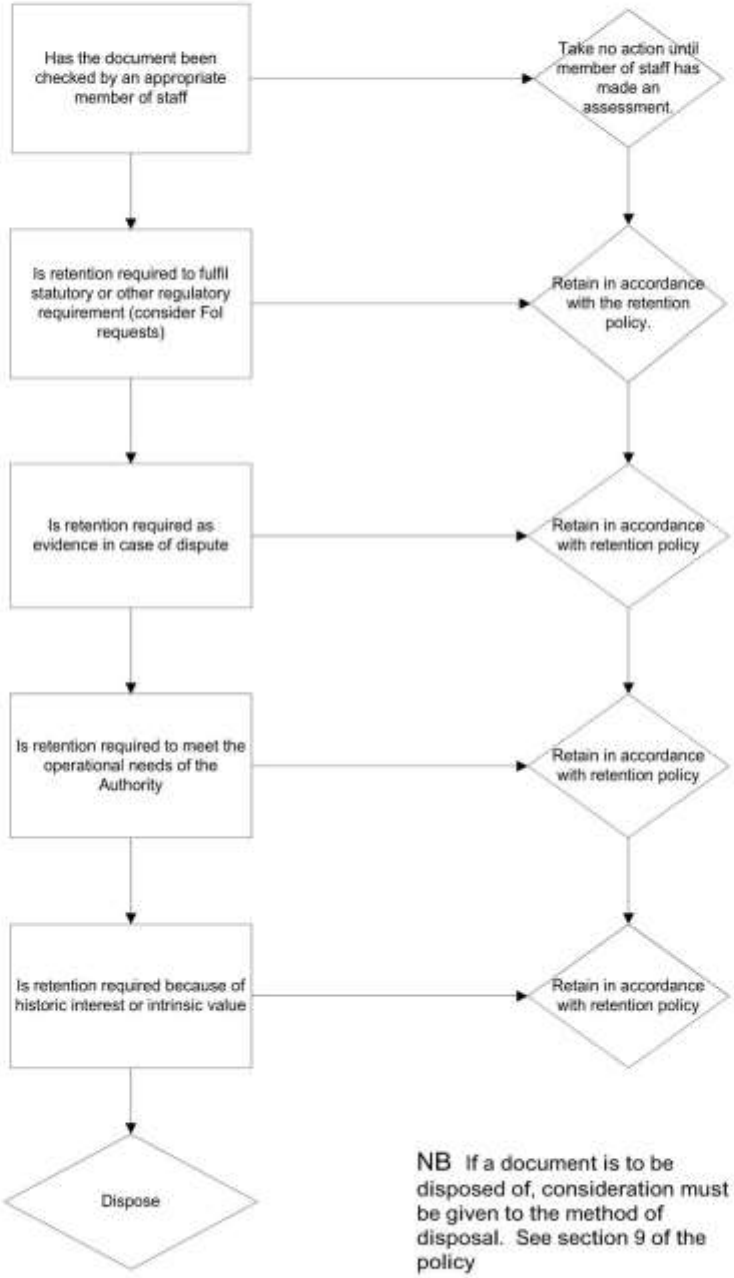
Emails stored in folders in staff Outlook accounts should be managed in the same way as documents held on the Authority's network drive. It is the responsibility of individual officers to ensure that any emails relating to business activity are saved in the relevant location on the network and not retained in mailboxes. Care should be taken with emails that contain personal data, including the email address of sender and recipient.

6. Deleting or Archiving?

At the end of the retention period, or the life of a particular record, it should be reviewed and deleted unless there is a sound business or legal reason for keeping it. There is a significant difference between permanently deleting a record and archiving it, but if a record is archived or stored offline, this should reduce its availability and the risk of misuse or mistake. However, personal information should only be archived (rather than deleted) if there is a requirement for it to be retained and which can be justified with reference to the GDPR. Records should also be deleted from the back-up. For the purposes of the Freedom of Information Act, data which exists on an archive but not on a live system is caught by the Act and therefore may have to be released.

Appendix A:

Should it stay or should it go: Key considerations for retaining or disposing of documents



NB If a document is to be disposed of, consideration must be given to the method of disposal. See section 9 of the policy

Records Management Policy V1.0

Annex B: Personal Data

This guidance should inform and help with decisions on the management of personal information as listed in the Information Asset Register]

The GDPR does not set out any specific minimum or maximum periods for retaining personal data, but is clear that personal data should only be retained for as long as is needed in relation to the purpose it was originally collected for –.

In practice, it means that the individual/Team/Service holding the personal data needs to:

- review the length of time the personal data is held – does it need to be retained for longer to meet a legal requirement, for example allowing an individual to make a claim related to injury after an event?
- consider the purpose or purposes for which the information is held in deciding whether to retain it - for example, next of kin details for volunteers should be retained for as long as the individual continues to volunteer;
- ensure that it is securely deleted or archived once it is no longer needed in relation to the purpose(s)
- consider whether it might be appropriate to anonymise the data which would allow the non-personal data to be retained and used for research and analysis
- On the flip side it's important to ensure that personal data is not deleted too soon; apart from disadvantaging our work, it may inconvenience the people the information is about. However, retaining personal data for too long may cause the following problems:

  - ✓ increased risk that the information will go out of date, and will be used in error
  - ✓ the passing of time makes it more difficult to ensure that information is accurate.
  - ✓ the personal data is no longer actively used, but must still be held securely.
  - ✓ difficulties in responding to subject access requests – we hold more data than necessary
  - ✓ breach of the GDPR and potential for monetary penalty issued by ICO
  - ✓ loss of trust of users and damage to our reputation

<u>So …things to remember:</u>

It's good practice regularly to review both the personal data and records we hold, and delete what we no longer need. Information that needs to be retained but not accessed regularly should be safely archived (perhaps with a local records office) or secured offline. Hard copy records containing personal data and/or confidential information should be securely shredded – for small amounts of data use the shredder on the copydeck, or speak with Property Service who can supply you with confidential waste bags.

If you're thinking about retaining personal data beyond the purpose for which it was originally collected, consider the following:

1. the current and future value of the information;
2. the costs, risks and liabilities associated with retaining the information; and
3. the ease or difficulty of making sure it remains accurate and up to date.
4. whether the retention is compliant with the GDPR - for example, in connection with a legal or contractual obligation or performance of a task carried out in the public interest.

Annex C – Retention Schedule

The current Retention Schedule is being revised but is available on the HUB for reference