The Authorised Retention and Disposal Policy Statement

1. Introduction

Information must be retained only for as long as it is required to support the Houses in meeting their business requirements and legal obligations, for reference or accountability purposes, or to protect legal and other rights and interests. At the end of that time, information will either be destroyed or transferred to the Parliamentary Archives for permanent preservation.

The Authorised Retention and Disposal Policy (ARDP) is the House Administrations' policy on the retention, destruction and archiving of its information. It supports the compliance of both Houses with legislation including, but not limited to:

- Data Protection Act 2018,
- Freedom of Information Act 2000, specifically the Code of Practice Section 46 (FOIA),
- Limitation Act 1980,
- as well as national and international standards.

The requirements outlined in this policy have been developed to provide a consistent approach to the retention and disposal of information. Retention periods and disposal instructions are produced in consultation with staff with primary responsibility for each business function and its related activities, plus other key stakeholders to establish and validate legal and regulatory requirements. Instructions are approved by the Senior Information Risk Owner (SIRO) for each House.

Related policies:

- Information Management Policy 2020
- Parliamentary Archives Collection Development Policy.
- House of Commons Data Protection Policy
- House of Lords Data Protection

2. Scope

Instructions in the ARDP apply to all physical and digital information, regardless of storage location or the media on which it is held.

Where information is held electronically within a database or other system, procedures must be put in place to ensure the systematic and authorised destruction or archiving of this material in accordance with the instructions outlined in the ARDP.

The ARDP relates to master copies of information – the official version retained for regulatory or business reasons. Where teams or staff hold copies of information, which they did not create and are not responsible for, these must not be kept for longer than the originals would be and can be routinely deleted.

1. **Back-ups -** Disposal of information/data on live systems will not include disposal on historic/business continuity backups. Backups will be retained for different lengths of time, depending on the criticality of the information/service and must be agreed as part of system set-up to ensure appropriate recovery times/retention periods. See PDS backup and Retention Strategy and Policy.

2. Publications - Historically the ARDP did not apply to published material as these were managed by the libraries of both houses. This changed in 2016 when Parliament's contract with TSO ended. In the digital world, the Archives will act as custodian of the record copies of Parliament's digital original publications, on behalf of the Libraries and others. The

Archives will work with the Libraries and other departments to ensure a convergence of requirements so that the Libraries can continue to access digital publications and to take paper copies where required. Teams with responsibility for creating and maintaining digital parliamentary publications must ensure these are included in the ARDP and work with the Parliamentary Archives to ensure copies of these are transferred for digital preservation. Note, it will be some time before the ARDP can reflect parliamentary publications in a comprehensive way.

3. Retention periods

The ARDP sets out how long information should be kept for (the retention period) and what should happen at the end of the that time (disposal instruction).

Retention periods are driven by business requirements and our legal obligations. If there is no legally defined retention period for information, it is the responsibility of the relevant business area to work with the Information and Records Management Service (IRMS) to determine an appropriate retention period.

Information must be disposed of as close as possible to the disposal date stated. There are a number of reasons for this:

- it is easier to identify what information is, or is not, available if disposal instructions are followed
- it is easier to pinpoint important information if redundant information has been removed
- storage (whether on a service, in the cloud or physical accommodation) can be used more efficiently
- principle 5 of GDPR states that personal data shall be kept for no longer than is necessary for the purposes for which it is processed
- if information exists in any form, it is discoverable under the Data Protection Act 2018 and Freedom of Information Act 2000.

4. Personal Data

Article 5 of GDPR requires that personal data must not be kept for longer than it is needed which is dependent on the reason for which the data was collected (business need). Personal data can be held for longer periods in certain circumstances, such as, public interest archiving, scientific or historical research, or statistical purposes. The ARDP directly supports the House Administrations' obligations under this principle to not keep personal data longer than needed.

Where personal data is held, this must not be retained in a form which enables identification of individuals for longer than is necessary to satisfy the purpose for which it was collected.

For information or data sets containing personal data, data anonymisation may be appropriate. This is the process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly. Personal data must be anonymise d if it is to be used for a purpose other than which it was collected (i.e. statistical purposes where the identity of an individual is not required). Anonymisation must be applied to all associated datasets and records, including any backups or copies of the information.

Information containing personal data may be selected for permanent preservation in the Parliamentary Archives. These are made available in accordance with the Freedom of Information Act 2000, as amended by the Data Protection Act 2018. Appropriate safeguards

must be put in place to minimise the amount of personal data needed for archiving purposes in the public interest.

5. Divergence from the ARDP

There are exceptions where divergence from the ARDP is appropriate in certain circumstances – for example, information relevant to a pending or actual legal dispute or action, investigation or inquiry, an active request under Freedom of Information or Data Protection legislation, an FOI Complaint which is subject to appeal, a change of legislation or regulations, or to support legitimate business needs. The Information and Records Management Service must be consulted on any divergence from the policy.

Where appropriate, information should be placed on legal hold. When information falls under a legal hold it should be clearly marked as such so it is not accidentally included in any scheduled destruction. If you are unsure whether information in your possession falls under a legal hold, contact the Information and Records Management Service or Legal Counsel for advice.

6. Implementation

Implementation is normally undertaken at a local level within business units. The Information Asset Owner should ensure that suitable methods are in place to store information in an appropriate manner which enables the identification of information as it reaches the end of its defined retention period as well as overseeing its disposal.

The Information and Records Management Service will work with business units to identify and execute disposal of information held in SharePoint sites.

7. Authorisation of disposal of information

Information must only be destroyed with the authorisation from the relevant Information Asset Owner (IAO). The IAO is the person responsible for the day-to-day risk management of the information, and is usually a senior manager in the relevant business area generating or holding the information who has an understanding of the context and risk associated with the information.

8. Recording disposal of information

Disposal of information must be documented to provide evidence of what has been disposed of, when, and who authorised the disposal.

This evidence must be maintained by the relevant team with responsibility for the information as it may be relied on in the event of a query or formal information request. Disposal authorisation may take the form of a list, register or summary appropriate to the process, plus supporting evidence as appropriate. Where possible, disposal of information in systems/databases should be recorded in system audit logs, which will supplement records of who authorised the disposal, and when.

9. Secure disposal of information

Information must be securely destroyed to a level that is commensurate with its sensitivity to prevent unauthorised access to, and later reconstruction or recovery of, that information.

Specific care must be taken over the disposal of any sensitive or personal data, as defined in the Parliamentary Protective Marking Scheme. The following secure methods of destruction must be adopted:

- Electronic information or data must be deleted in a way that ensures information cannot be retrieved or reconstructed.
- Information on hard drives, removable media and any similar items must be securely era sed before disposal or reassignment of the equipment.
- Where information cannot be erased from equipment, it must be physically destroyed by an authorised, specialist destruction company, and certificates of destruction obtained.
- Paper copies of information marked Restricted or above must be destroyed using cross-cut shredders or disposed of securely as confidential waste by an approved third party.

10. Transfer to the Parliamentary Archives

Instructions in the ARDP work alongside the Parliamentary Archives Collection Development Policy (CDP) to identify information with long term historic value which must be retained permanently and transferred to the Parliamentary Archives. However, it cannot cover all circumstances and the Parliamentary Archives will appraise and sample records against the criteria in the CDP where appropriate to ensure identification of landmark moments, events or Parliament's responses to them and enable the timely transfer of material whether that be in hard copy or digital format.

11. Updates to the ARDP

The Authorised Retention and Disposal Policy is not a static policy and its maintenance is an on-going task. It will be regularly updated to reflect:

- Changes in legislation or regulations
- Changes to business functions or processes
- Changes in format and systems
- New types of information created
- Superseded or out-of-date terminology

Staff are able to propose additions or changes to the ARDP at any time by contacting the Information and Records Management Service. Significant changes will require consultation with other relevant teams and approval by the Senior Information Risk Owners.

12. Using the ARDP

The ARDP is arranged into areas representing business functions, rather than by team or office. A functional approach ensures that the Policy does not need to change in the event of organisational restructures and that information held by multiple teams is only captured once.

Generally, the information a team hold will not span across all areas, and you will only need to refer to specific functions which relate to your work.

- Each function area includes a short scope note explaining what the term covers.
- Each function area is organised into the activities carried out as part of that function. Additional terms are used to further define sub-processes or activities of information where appropriate.
- Examples of the types of information covered by a disposal instruction are provided under each term. The examples given are illustrative only, and not intended as an exhaustive list of all types of records, documents and data which may be created as part of that activity term.
- Details of how long information should be retained, and how it should be disposed of is provided against each term.

- A reason for this retention period is also provided, including business, historical and legislative factors.

Responsibilities

- IRMS
    - Are responsible for managing corporate, bi-cameral information management policies, including the ARDP and advising users on their responsibilities and implementation of policies.
- Record Officers
    - Record Officers are the first point of contact for information management in their business area. They should be familiar with which areas of the ARDP apply to their information and be prepared to act as liaison with colleagues and IRMS regarding any changes to the policy.
- IAOs
    - Information Asset Owners protect and manage Parliament's information assets. As well being aware of information created and used, where it is stored and how it is managed in their business area, they should also authorise disposal in accordance with the ARDP when necessary. IAOs should also work with IRMS to ensure the ARDP is up to date and reflects the information they create and manage in their business areas.
- Solution/Service Owners
    - Solution/Service Owners are accountable for the quality of a function, service, programme or project who takes business decisions in direct response to information risk. They are responsible for ensuring retention requirements in line with the ARDP are considered for any new service or solution and its associated processes.