# Information Management Policy

## Document Control

| | |
|---|---|
| **Title** | Information Management Policy |
| **Approved by** | Senior Information Risk Owners |
| **Date of approval** | 28/10/2024 |
| **Review frequency** | Annually |
| **Next review date** | October 2025 |

## Version history

| Version | Date | Prepared by | Reason |
|---|---|---|---|
| 1.0 | November 2020 | Head of Information and Records Management | To replace the Information and Records Management Policy 2014 |
| 1.1 | October 2024 | Head of Information and Records Management | Sections on handling SECRET information updated. Minor updates to reflect publication of Information and Digital Strategy, establishment of the Information and Digital Board and other organisational changes. Formatting updated to make document more accessible. |

Any queries about this policy should be sent to the Information and Records Management Service.

## Contents

## 1. Policy Statement and Purpose

Information is central to the work of Parliament. It provides a full and accurate record of the House Administrations' activities, and informs scrutiny, research, decision making, and policy development. The Houses are responsible for a large amount of information, which must be managed to ensure good governance, deliver services efficiently, manage risk effectively, and comply with legal and regulatory obligations.

This policy provides a framework for managing each House's information, covering storage, access, protection, retention and disposal of information, regardless of format. It sets out the expectations on staff in fulfilling their duty to manage information responsibly and the responsibilities of different teams, groups and roles which directly support implementation of the policy. It also reflects relevant legislative requirements, international standards and best practice approaches for the management of information by public bodies.

## 2. Scope

This policy applies to all recorded information created, received, and maintained as evidence or an asset by the Administrations of the House of Commons, the House of Lords or both Houses, including the Parliamentary Digital Service, in pursuit of legal obligations or the transaction of business ("parliamentary information").

This includes information relating to core parliamentary activities in the Chambers and Committees, as well as that relating to wider supporting activities such as finance, digital services, security and estates management. Examples include, but are not limited to:

- Documents and data (both structured and unstructured) held in digital systems, including parliamentary supplied systems and devices, in applications and software used on personal devices, and external web-based collaboration platforms.
- Emails, chats, instant messages, and text messages (including WhatsApp, Messenger etc).
- Hard copy information and files.
- Audio and video recordings, photographs, animations and multimedia content.

- Building maps, plans, and 3D models.
- Social media (including posts on platforms such as Facebook, X, Instagram etc).
- Content related to the development of parliamentary publications (e.g. drafts prior to publication) and the final digitally published versions.[1]

For the purposes of this policy, no distinction is made between documents and records. All parliamentary information is subject to the policy irrespective of how it is categorised. This policy also notes that the House of Commons and the House of Lords are separate controllers.

## 3. Out of scope

This policy does not apply to:

- Information processed on parliamentary systems on behalf of another controller, e.g.:
    - Information and communications by Members of the House of Commons and their staff with or about constituents.
    - Non-parliamentary pensions.
    - Workplace Equality Networks.
    - Information and communications created by staff acting in their role within a trade union.
    - Groups such as the Commonwealth Parliamentary Association and the British-Irish Parliamentary Assembly.
    - All-Party Parliamentary Group activities.
- Personal or non-work-related information which pertains solely to an individual's domestic affairs held on parliamentary systems, as per Parliament's Acceptable Use User Responsibilities.
- External materials acquired and kept solely for reference.
- External publications maintained by the Libraries of each House.

[1] In the digital world, the Archives act as custodian of the record copies of Parliament's digital original publications, on behalf of the Libraries and others.

## 4. Who the Policy applies to

Parliamentary information is the property of its respective House Administration and individuals and teams entrusted with its custody are expected to manage it appropriately. This policy therefore applies to all staff in both Houses, including permanent and temporary staff, and extends to contractors, consultants, secondees and volunteers undertaking work on behalf of either House. Contract Managers must also work with third parties to ensure they understand their obligations in receiving, handling, storing and disposing of parliamentary information in the course of executing their contracts.

Members who hold an official position within a House Administration (e.g. as a Chair of a Committee) must follow this policy, but only in relation to the information that they create and use in carrying out that role.

## 5. Specific Roles and Responsibilities under this Policy

**All staff** (including contractors, consultants, secondees and volunteers) must:

- Take personal responsibility for the effective management of information.
- Create full and accurate records of their work.
- Store information in approved, shared systems so that it is accessible by colleagues.
- Protect information from loss or unauthorised access.
- Retain and dispose of information in accordance with policy.
- Ensure information they have created, received or been responsible for in the course of their work remains accessible when leaving their role or Parliament.

**Heads of teams or business units** must take all reasonable steps to ensure that information management policies and procedures are followed by users. They must ensure appropriate resources exist within their area to fulfil responsibilities for managing information.

**Record Officers** are the link between the business and the Information and Records Management Service (IRMS). They help colleagues in their team/office to adhere to information management policies by providing local guidance, communicating messages and disseminating guidance, and acting as the first point

of contact for colleagues who have queries, as well as having specific responsibilities for their team's SharePoint sites and associated Microsoft 365 applications.

**Information Asset Owners** are responsible for the day-to-day assessment and mitigation of risks to information assets. This includes ensuring these are adequately secured and protected, shared, reused, and published where appropriate, and that disposal of information assets is authorised.

**Departmental Information Risk Owners** (**DIROs**) in the House of Commons and **Information Security Coordinators** (**ISCs**) in the House of Lords have responsibility for information risk assessment, monitoring, and mitigation within their team or business unit. They provide assurance to their respective SIRO or Head of Office that risks have been identified and addressed and that business practices accord with policies and guidance.

The **Senior Information Risk Owners** (**SIRO**) are responsible for information risk in their respective House, and approve information related policies.

The **Information and Digital Board** provides strategic leadership for information, data and digital matters in Parliament. It promotes a positive culture across Parliament around information management and maintains oversight of information risk. It is a sub-committee of, and reports to, the House of Commons Executive Board and the House of Lords Management Board.

The **Information and Records Management Service** (**IRMS**) is responsible for managing corporate, bi-cameral information management policies, advising users on their responsibilities and implementation of policies, providing training and guidance, assessing compliance, and supporting the network of Record Officers.

The **Parliamentary Digital Service** supports identification and implementation of information management and security requirements when working with the business to procure, develop, implement and decommission systems and services which hold, create or process information.

The **Risk and Assurance Working Group** works with Information Asset Owners and system owners to manage information risks that are within the scope of the Bicameral Information Risk Appetite Statement, including accreditation of systems and services, and raises any risks that fall outside of that Statement to the SIROs.

The **Information Strategy and Governance** (**ISG**) team provides the secretariat function to the Information and Digital Board, supports the SIROs, and co-ordinates and monitors delivery of the Information and Digital Strategy and associated actions.

**Parliamentary Knowledge and Information (PKI)** supports Parliament to manage its information and archives securely, transparently and lawfully, including preserving evidence of Parliament's work through its archive.

The **Information Compliance teams** are responsible for compliance with information rights legislation, (including Freedom of Information and Data Protection) in their respective House and investigating information losses/personal data breaches.

The **Information Security Team** are responsible for maintain the Bicameral Information Risk Appetite Statement, managing the accreditation and assurance of systems and raising awareness of information security risks.

## 6. Policy Requirements

The following requirements define key concepts and principles from which detailed rules, controls, processes and systems for managing information can be developed. They establish a baseline standard of good practice and compliance for application across the Houses' wide variety of procedural and technical environments.

### 6.1 Creation

Users must create and keep information which enables the effective delivery of the Houses' operations and services, acting as full and accurate evidence of communications, decisions made, actions taken, and authorisations given.

- Business units must establish what information must be created to fully document their activities, taking into account the operational, legislative and regulatory environment.
- The Houses will aim to maintain a single, authoritative source of the truth, which is shared appropriately and reused across different service areas. Users must avoid creating or keeping duplicates of information.

### 6.2 Storage: Digital information

Information will be captured and maintained in such a way that it is readily identifiable, accessible and retrievable at all times throughout its lifecycle, in a manner that is proportionate to the value and sensitivity of that information.

- Relevant and proportionate information management requirements will be included in the design and configuration of systems which hold or process digital information to ensure information can be found, accessed, used, understood, trusted, and kept for as long as it is needed. This will include metadata (i.e. descriptive and technical documentation) that ensures the integrity of the information as a corporate asset, and application and execution of disposal instructions (including migration and/or export to another system).
- Users must only store digital parliamentary information on corporately approved or accredited systems where it is available to other, authorised users. On occasions where this has not happened, Information Asset Owners must arrange for information to be transferred out of the system (if required) and erased.

- The primary corporate system for unstructured documents and information is SharePoint.
- Users must not store parliamentary information on personal devices, non-PDS issued removable media, or send it to or store it in personal email, cloud storage, or social media accounts. Parliamentary supplied personal spaces such as OneDrive must not be used to store the only copy of parliamentary information, apart from certain line management information or very early drafts.
- SECRET information will only be held digitally in exceptional circumstances, on assured digital systems approved and accredited for this use. Do not store SECRET information on Parliament's normal Microsoft 365 cloud-based storage (e.g. SharePoint, Outlook, Aconex, HR, Finance or other systems) or on personal devices.
- Parliament does not recognise social media (e.g. X, Facebook), messaging applications (e.g. Whatsapp, Messenger) or free web-based platforms (e.g. Trello, DropBox, Slack) as appropriate systems for storing information in line with this policy (except in approved and limited circumstances). As far as possible, parliamentary suppled Microsoft 365 tools should be used for these purposes. Information held on these applications is covered by the Freedom of Information Act and Data Protection legislation and must be available to be considered for disclosure.

### 6.3 Storage: Hard copy information

Information will be stored in hard copy only where this is required for evidential, historical or legal purposes, or it is not practical, efficient or economical to digitise the originals. Equipment used to store hard copy information must be secured in accordance with the Parliamentary Protective Marking Scheme and appropriately protected from fire, water ingress, and other hazards.

### 6.4 Organisation and Control

The Houses will put in place controls to establish what information they hold and where in order to be able to understand its value and manage it appropriately.

- Business units must maintain Information Asset Registers and, for personal data, Registers of Processing Activities, which describe what information

assets they hold, where these are held, who the information asset owner is and general arrangements for access and security.

- Business units must maintain registers of hard copy information, including tracking systems for the movement of sensitive information.
- Users must save information in such a way that it can be easily located by others now and in the future, using clear, meaningful, and consistent names, and applying additional descriptive metadata where mandated.
- The Houses will maintain a Classification Scheme which describes what information the House Administrations create and receive in the course of their business, and provides a framework through which access, security, and disposal policies can be applied.

### 6.5 Access and Sharing

The Houses promote a working culture of openness and collaboration. Parliamentary information that is not sensitive will be accessible to all staff and be restricted only when there is a business need to do so (e.g. personal data, security, commercially sensitive). Sensitive information will be defined as per the Parliamentary Protective Marking Scheme for the period that it remains sensitive.

- Technology planning must take access permissions and information sharing in digital systems into account.
- Information Asset Owners must ensure that appropriate technical and organisational measures are put in place to protect information against unauthorised or unlawful access and accidental loss or destruction.
- Access controls to information must be proactively monitored, and steps taken to remedy incorrect application or update these controls if the level of sensitivity of the information changes.
- All users must be security cleared to a level appropriate to the sensitivity of the information they will be handling.
- Users must share information via links, whenever possible, to mitigate the risks of working from out-of-date copies and information being over-retained in breach of policy.
- Users must report information losses and breaches of information security as soon as they become known so that they can be investigated and monitored.

- Where parliamentary information or personal data is shared with or created by third parties, agreements or GDPR compliant contracts that set out what information is shared, how it can be used, how it should be handled and arrangements for its security and safeguarding must be put in place prior to the information being shared, if such an agreement does not already exist. There will be exceptions to this where information is published or made available via the Open Parliament Licence.

### 6.6 Protective Marking and Handling

Parliamentary information will have a protective marking to inform users of the level of protection required when creating, sharing, and re-using information. The Parliamentary Protective Marking Scheme (PPMS) is the House Administrations' policy which sets out how information of different sensitivity levels should be marked and handled.

- Users must apply or note a protective marking to ensure the safety and security of sensitive information.
- Users must handle protectively marked information in a manner that is appropriate to the information's sensitivity.

Users must proactively monitor information assets' markings and review whether those markings are appropriate.

### 6.7 Evidential Weight

The Houses will put in place controls to ensure that parliamentary information can be relied upon as authoritative, authentic and having integrity.

- Hard-copy information that is scanned with the intention of destroying the original will be scanned to a standard that ensures legal admissibility.
- Appropriate version control procedures should be used to ensure that superseded versions of information are retained in accordance with relevant legal requirements, business needs and the Authorised Retention and Disposal Policy (ARDP).
- Audit trails of activities relating to parliamentary information in digital systems will be created and steps taken to protect them from accidental or malicious access, alteration, or loss.

## 6.8 Disposal

Information will 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. Where personal information is held, this will not be retained for longer than is necessary to satisfy the purpose for which it was collected.

The Authorised Retention and Disposal Policy (ARDP) is the House Administrations' policy on how long information should be kept for and how information should be disposed of.

- Information must be retained and disposed of in a timely fashion, in line with instructions in the ARDP only. This includes data in line of business systems and databases. Where no suitable instruction can be identified, advice must be sought from the IRMS.
- Users must not dispose of parliamentary information without authorisation from the relevant Information Asset Owner.
- 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.
- Disposal of information must be recorded to provide evidence of which information has been disposed of, when that disposal occurred, and by whom that disposal was authorised. Information that is due for destruction but related to an ongoing information request, legal proceedings, regulatory investigation, or audit must not be destroyed until the matter, including any complaint or appeal, has been closed. It is an offence under information laws to erase or destroy data with the intention of preventing disclosure in response to a request for information.
- Teams with responsibility for creating and maintaining digital parliamentary publications must work with Parliamentary Knowledge and Information to ensure copies of these are transferred for digital preservation.
- Where information is shared with or created by third parties, agreements or contracts must be put in place that ensure those organisations either return

information to Parliament's custody or dispose of it in line with policy and provide confirmation of that disposal upon request.

- Information selected for permanent preservation as part of Parliament's archive will be transferred in the form in which it was created for business purposes, unless explicitly agreed otherwise.

## 7. Monitoring Compliance

Compliance with this policy will be monitored and local controls for managing information assessed to ascertain their effectiveness. This may include checks on contractors or third parties holding parliamentary information. It should also include regular system reporting and audits to monitor security of information and adherence to information policies. The IRMS will support teams to develop action plans to improve any identified weaknesses. Serious violations of policy or significant risks or issues will be escalated to the relevant SIRO.

## 8. Assurance

This policy and related policies and processes provide controls for the management of information risks. The Accounting Officers (the Clerk of the House in the House of Commons and the Clerk of the Parliaments in the House of Lords) will report on the effectiveness of those controls in their Annual Governance Statements.

Teams and offices must provide the Accounting Officers with self-assessments of local controls for managing information as part of annual assurance processes.

## 9. Learning and Skills Development

Induction materials, training and guidance will be made available to enable users to carry out their responsibilities as outlined in this policy. Training offerings will be delivered in a variety of formats, appropriate to the levels of responsibility of the intended audience and cater to different learning styles.

Heads of teams or business units must ensure that all users undertake basic information management and security training as appropriate to their role.

## 10. Organisational and Technological Change

Information management issues must be given due prominence during significant organisational change (whether internal restructures, the creation and transfer of

powers to new bodies, or transformational ways of working programmes). Where information is formally transferred to a separate data controller, agreements should include reference to information ownership, retention periods and related considerations.

All new technology solutions must be assessed via the accreditation process to ensure that the effective management and security of information is built in to both the system, and associated processes, prior to implementation. Owners of digital tools or solutions must ensure these tools meet policy requirements and that controls in place are still appropriate during operation and management of information is considered when tools are decommissioned.

## 11. Policy Approval and Review

This policy has been approved by the Senior Information Risk Owners and will be regularly reviewed to maintain its currency.

## 12. Annex A

This policy works alongside a variety of parliamentary policies and guidance documents related to the management of information. This policy should be read in conjunction with:

- Bicameral Information Risk Appetite Statement
- Acceptable Use User Responsibilities
- Parliamentary Protective Marking Scheme
- House of Commons and House of Lords Data Protection Policy Statement.
- Authorised Retention and Disposal Policy
- Archives' Collection Development Policy
- Restoration and Renewal Parliamentary Relationship Agreement and Data Sharing Agreement.

## 13. Annex B

This policy is written with reference to the following legislation and standards:

- Freedom of Information Act 2000 and the Code of Practice on the Management of Records under Section 46 of the Act.
- The General Data Protection Regulation, as supplemented by the Data Protection Act 2018.
- Environmental Information Regulations 2004.
- ISO 13008: 2012 Digital records conversion and migration process.
- ISO 14721: 2012 Space data and information transfer systems – Open archival information system (OAIS) – Reference model.
- ISO 15489 Records Management.
- ISO 16175-2:2011 Principles and functional requirements for records in electronic office environments.
- ISO 16363: 2012 Space data and information transfer systems – Audit and certification of trustworthy digital repositories.
- ISO 23081-1: 2017 Records management processes – Metadata for records.
- BSI DISC BS10008 Evidential weight and legal admissibility of electronic information.
- BS 10010:2017 Information classification, marking and handling.
- BS 15173 Secure destruction of confidential material.