HOUSES OF PARLIAMENT

Parliamentary Information & Records Management Policy (v3.0) 2014

This policy has been prepared by the Information and Records Management Service of the Parliamentary Archives, approved by the Clerk of the Parliaments and Clerk of the House and circulated to the Management Boards of each House. It is effective from December 2014 and supersedes the *Parliamentary Records Management Policy 2006.*

The *Parliamentary Information & Records Management Policy* v 3.0 contributes to strategic aims relating to the efficient management and use of information to support delivery of corporate services, foster informed decision making, facilitate accountability, transparency and collaboration, and preserve and ensure access to information and records for the benefit of present and future generations. It provides the framework for the ongoing development of procedures, tools and systems for the effective management of information across the House of Commons and Lords administrations and PICT.

Copyright Statement

Document control

Author:	Information & Records Management Service
Owner:	Director of the Parliamentary Archives
Approval:	Clerk of the Parliaments and Clerk of the House
Date Approved:	
Document Number:	V 3.0

Revision History

Version	Date	Summary of Changes
1.0	2000	
2.0	2006, April	Policy revised to bring it in line with the Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000
3.0	2014, March	Policy revised to take account of EDRMS implementation and other technological and business changes and to bring it in line with the revised and reissued Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000 (July 2009)

1. Policy Statement and Purpose

Parliament recognises that information is a valued corporate and public asset (i.e. information asset). Every organisation has controls to manage its assets: some are mandatory, others are part of good management practices. Both Houses of Parliament are responsible for large amounts of information and content, and both are adopting digital by choice as their way forward. The effective management of this information and content is an integral element of good governance and risk management. The aim of this policy is to provide a framework for managing each House's information and content (i.e. data, documents, records and other recorded information that has a specific content and a value to Parliament) – henceforth referred to as *information and records management*.[1] It will enable the House administrations to:

- deliver quality services to Members, the public and others by having timely access to authoritative and appropriate information about activities that can be retrieved, used and relied upon in current business
- increase efficiency and cost-effectiveness by ensuring that information and content is disposed of when no longer needed, enabling more effective use of resources (e.g. space within buildings and information systems) and saving staff time searching for information that may not be there
- comply with legal obligations or best practice which requires information to be kept, controlled and accessible (e.g. Data Protection Act 1998, employment legislation and health and safety legislation)
- improve accountability, enabling compliance with legislation and other rules and requirements to be demonstrated to those with a right to audit or otherwise investigate the organisation and its actions
- make sure we are open, transparent and respond appropriately to information requests, enabling protection of the rights and interests of an authority, its staff and others
- protect information vital to the continued functioning of each House in support of business continuity
- promote our achievements
- provide institutional memory, contributing to Parliament's heritage. [2]

Legislation increasingly underlines the importance of good information management, in addition to sound business practice. Compliance with acts such as the Freedom of Information Act 2000 and the Data Protection Act 1998 is underpinned by effective information and records management.

This policy demonstrates the Houses' recognition of information and records management as a specific corporate activity and its commitment to complying with relevant legislation, international standards and best practice approaches for the management of information by public sector bodies[3]. It also recognises the role good information and records management plays in mitigating risks including:

- Poor decisions based on inaccurate or incomplete information
- Inconsistent or poor levels of service

[1] See Section 4 for a list of the information assets not covered by this policy.

[2] Derived from *Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000*, p.5.

[3] See Appendix 1.

- Financial or legal loss if information required as evidence is not available or cannot be relied upon
- Non-compliance with statutory or other regulatory requirements, or with standards that apply to Parliament's work
- Failure to protect vital information, leading to inadequate business continuity planning
- Unnecessary costs caused by storing information for longer than it is are needed
- Staff time wasted searching for data, documents and records
- Staff time wasted considering issues that have previously been addressed and resolved
- Loss of reputation as a result of all of the above.[4]

This policy is supported by a set of information and records management standards which:

- Define how corporate information must be managed
- Enable compliance with existing and evolving information and records management across both administrations to be measured
- Enable identification and promotion of good practice
- Support the increased use of digital assets as a means of gaining organisational benefits without introducing additional risks.

2. Good Practice Principles

Good practice will be achieved by:

- **Managing information effectively as a strategic parliamentary resource.** Information resources, regardless of where they are held, are corporate resources. They are the property of the relevant House(s) and PICT and not of individual staff or teams.
- **Determining responsibility for Parliament's information assets.** Those with specific responsibility for managing business information must be clearly identified. However, all staff are accountable for the use and handling of information.
- **Sharing information responsibly with our colleagues, Members and the public.** Staff should be able to access information for the effective performance of their role. There should be the opportunity for the free flow of information, where appropriate, across the House administrations and PICT to facilitate the use, reuse and repurposing of it.
- **Protecting information**, especially personal information (e.g. personal data, draft committee reports, information sensitive for security or commercial reasons).[5]
- **Producing accurate information.** Corporate information must be timely, relevant and consistent, with duplication kept to a minimum.
- **Maintaining our information in compliance with this policy and our statutory and business obligations.**
- **Retaining information only for as long as it is needed, and disposing of it only in accordance with corporate policy.**

3. Glossary

Archive*:* Information that has been determined to have sufficient historical, administrative, legal, fiscal, or other value to warrant permanent preservation by the Parliamentary Archives.

[4] Derived from *Code of Practice*, p.5.

[5] Please refer to *Your Role in Safeguarding Information: A Guide for Staff of either House & PICT*.

Classification*:* systematic identification and arrangement of business activities and/or information into categories according to logically structured conventions, methods and procedural rules represented in a classification system.

Corporate information system**:** a system, computer-based or other, for collecting, storing, and processing data and documents and for delivering information, knowledge, and digital products.

Data: Symbols or characters that represent raw unorganised facts or figures and form the basis of information; data is often used to refer to information in its most atomised form and is independent of any medium in which it is captured. Data is intangible until it has been recorded in some medium.

Database: A digital file that stores structured data.

Disposal*:* the processes associated with implementing information retention (i.e. destruction, deletion or archiving), which are documented in the *Authorised Records Disposal Practice*.

Information: a term used to cover data, documents, records and other recorded information that has a specific content and a value to Parliament, i.e. there would be a consequence if you could not produce it for legal, financial, reputational or operational efficiency reasons, or risk if it were to be lost, inaccurate, tampered with or inappropriately disclosed.

Information asset: a body of information grouped into manageable portions so that it can be understood, shared, protected and exploited effectively. ‘Manageable portions’ are defined at a level of detail that allows its constituent parts to be managed usefully as a single unit; assessing every individual file, database entry or piece of information isn’t realistic. Information assets have recognisable and manageable value, risk, content and lifecycles.

Information life cycle: the life span of information from its creation or receipt to its final disposition (i.e. destruction or transfer to the Parliamentary Archives).

Record*:* information, irrespective of format or the media on which it is held, created, received and maintained as evidence and information by both Houses, in the transaction of business or in pursuance of legal obligations. *Although this term is defined here, the distinction between records and documents or records and information has become increasingly arcane under current legislation (e.g. the Freedom of Information Act 2000).*

Recorded information: defined as any feature or characteristic of a document that imparts information or knowledge to the viewer. This means that the term ‘recorded information’ doesn’t just apply to the text; it covers any component of the document that conveys information, for example: design and layout (which can reveal if it is a report, spreadsheet or letter), logos and letterheads (indicates to some degree the authenticity and legitimacy of the information), language (e.g. the tone), emphasised wording (e.g. use of underlining, italics or bold font indicates the significance of the emphasised words), handwriting, annotations, headers and footers, images and email transmission details.[6]

[6] The Information Commissioner’s Office’s broad interpretation of ‘recorded information’ reflects the view taken by the Upper Tribunal in Independent Parliamentary Standards Authority (IPSA) v Information Commissioner and Leapman UKUT 0033 (ACC) (23 January 2014).

4. Scope

This policy applies to all recorded information, irrespective of format or the media on which it is created, received, held and maintained as evidence and information, in the transaction of business or pursuance of legal obligations. It includes emails produced or received in the conduct of business, data held in both structured and unstructured systems and applications (both on the Parliamentary Estate, on personal or mobile devices and outsourced, e.g. to the Cloud), as well as hard copy information, web content, audio and video recordings, maps and plans, photographs, text messages, wiki pages and blogs, and social media posts. Some systems distinguish between documents and records, however any recorded information held by the House administrations is subject to the provisions of this policy irrespective of how it has been categorised.

This policy does not relate to:

- External publications maintained by the Libraries of each House that do not need to be retained permanently by the Parliamentary Archives[7]
- Information processed on behalf of another data controller (e.g. non-parliamentary pensions work, security clearances for IPSA staff)
- Non-work related information, including information held by staff acting in their role within a trade union
- Library and other materials made or acquired and preserved solely for reference
- Stocks of blank forms or templates
- Copies of vendor catalogues and product literature

Parliamentary information is the property of the relevant House administration or PICT. Individuals and teams entrusted with its custody are expected to manage it appropriately.

As a result, this policy applies to all Departments, Offices and staff of the administrations of both Houses of Parliament and PICT (both permanent and temporary including employees, contractors, consultants, secondees or volunteers undertaking work on behalf of either House) who have access to Parliamentary information, whether digital, paper or audio-visual.

It further includes information managed on behalf of the House administrations and PICT by an external body such as a contractor. Ownership, management and custody requirements should be articulated as part of any contract entered into by either House with an external party, where that party performs a function or service on behalf of the House.

Members, where they hold an official position within the administration (e.g. as a Chair of a Committee), are also subject to this policy, but only in relation to the information created and used in carrying out this role.

5. Accountability

All staff, contractors, consultants, secondees, volunteers and Members holding official positions within the administrations (‘information users’) are responsible for:

- taking personal responsibility for the effective management of information
- creating full and accurate records of their work

[7] In the digital world, the Archives will act as custodian of the record copies of 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 are able to continue to access digital publications and to take paper copies where required.

- capturing information in approved systems (either digital or hard copy)
- applying appropriate security and access controls
- retaining or disposing of information in accordance with corporate policy
- ensuring information for which they are responsible remains accessible when leaving their role or Parliament

The Librarian & Director of Information Services in the House of Lords, and the Senior Responsible Officer and budget holder in the Commons are responsible for agreeing strategic direction and ensuring that policies and processes are in place for the safe management of information.

The Parliamentary Archives is responsible for providing an information and records management service and an archive service for both Houses of Parliament, including producing related policies, standards, procedures and guidance, advising colleagues on their information and records management responsibilities (digital and paper) and supporting a network of Record Officers to liaise with the Archives and carry out work at a local level. The Archives also has responsibility for monitoring compliance with policies. This work is carried out by the Information and Records Management Service (IRMS) of the Parliamentary Archives.

Heads of Departments/Offices are responsible for:

- assigning information and records management roles and responsibilities e.g. Record Officer, authorising officer for disposal of records etc.
- overall adherence to information and records management in their area of responsibility, ensuring appropriate action is taken to address any shortcomings
- owning the risk of failure to manage information as required
- requesting information and records management audits and health checks
- considering information management implications when planning to commission new systems or undertake major structural or technical changes

Information Asset Owners will be responsible for the day-to-day assessment and mitigation of risks to a set of information assets, including ensuring that the disposal of information assets is authorised.

Line Managers are responsible for ensuring their staff are aware of their information and records management responsibilities and arrangements for access to information, as well as which systems should be used to store information. They must also allow staff the appropriate time and resources to manage information in line with corporate policy and practice and, where appropriate, include information and records management responsibilities in job descriptions, annual appraisals and development reviews.

Record Officers are the link between the business and the Information and Records Management Service (IRMS). Appointed by their Head of Department/Office they have responsibility for:

- liaising with the IRMS to ensure compliance with policies and procedures in their area
- providing advice to staff on the local application of policy and practice
- training new staff on local information and records management practices and procedures
- reporting to the Head of their business unit areas of non-compliance and other issues as they arise

6. Building Capability

Since all information users are involved in creating, maintaining and using information, it is important that everyone recognises information as an asset and understands their responsibilities as set out in this policy. Training, guidance and other relevant communications will be made available by the IRMS in a variety of formats suitable for all learning styles, and appropriate to the level of all staff responsibilities outlined in this policy.

7. Policy Implementation Framework

Parliamentary information must be managed through its lifecycle: from creation, through to storage, use and disposal. This policy will be implemented through the creation of guidelines and procedures developed by the IRMS, in consultation with appropriate members of staff.

Information and records management requirements must be integrated with technology planning and strategy to ensure that digital information is accessible and usable over time, despite technological change. Where new technologies will hold business information, consideration must be given to how it will be managed to meet the core principles for managing information as set out in this policy, namely:

7.1 Creation

All information users have a responsibility to create full and accurate records of their work, documenting information communicated, decisions made or actions taken. Departments/Offices must take into account the operational, legislative and regulatory environment in which both Houses operate when identifying what records must be created to fully capture evidence of their activities.

7.2 Capture

The majority of current information is captured digitally. It can be found in a variety of systems and locations, in many formats and on different media.[8]

It is important that information is captured and maintained in such a way that it is readily identifiable, accessible and retrievable at all times throughout its lifecycle.

7.2.1 Corporate applications and information stores

Departments/Offices must ensure that staff are aware of which systems should be used to store and manage parliamentary information. Staff must make certain that all information created and received by them as part of their work is captured within an appropriate corporate application or information store (e.g. HAIS (HC), MyHR (HL), SPIRE, Data.parliament), or moved to an appropriate system. The corporate electronic document and records management system (EDRMS), SPIRE, together with Parliament's digital preservation system enable us to store and preserve most records digitally, instead of on paper. As a result, records should be held in electronic form for most purposes.

Information held in SPIRE does not have to be printed and filed in hard copy. Information held in other information stores (e.g. shared network drives, corporately provided personal storage spaces

[8] Please note that all work-related recorded information is subject to disclosure under the Freedom of Information Act 2000, Data Protection Act 1998 (if personal data) or the Environmental Information Regulations 2004 (if environmental information) regardless of where it is held or how it is accessed, including on non-work personal email accounts or personal mobile devices (e.g. parliamentary or an individual's laptop, mobile phone, tablet, home PC), or in any other media.

including OneDrive, collaboration applications such as SharePoint and parliamentary email accounts) must either be moved into SPIRE as soon as it is useful to do so or printed to paper and filed in corporate file covers, deleting it at source afterwards. Failure to do so may result in information being outdated, incomplete or inaccurate, duplicated, not kept, not found when needed, wrongly disclosed or wrongly destroyed.

Provisions for storing information in other corporate applications will vary. Consult the IRMS about requirements for information held in strategic 'line of business' systems (e.g. HAIS (HC), MyHR (HL)), on the intranet or Content Management Systems (CMS) and Data.Parliament, in externally hosted software applications, or 'cloud' systems.

Some hard copy information is still held; it is often retained where an original copy of a document is required for evidential purposes (e.g. property deeds), or where the format of the information makes it unsuitable for converting to digital format (e.g. large scale maps and plans). Storage accommodation for hard copy records in offices and in off-site facilities should be clean, tidy and secure, and should prevent damage to the information. Equipment used must be safe from unauthorised access and meet fire regulations, but also allow maximum accessibility to the information commensurate with their frequency of use. Recorded information held as archives in the Victoria Tower repository are preserved according to BSI standards.

7.2.2 Non-corporate applications and information stores

Information should not be held outside corporate applications or information stores, except as temporary off-line copies needed to work off-site or off-line.

Sensitive and/or personal information must never be held outside corporate applications or information stores, even as temporary off-line copies. If stored outside corporate control, information is at greater risk of unauthorised access, loss, intentional or accidental alteration or destruction, and compromises the House administrations' ability to account for the information they hold and the way in which that information is used and managed.

Parliamentary information might also be found in a range of alternative locations such as:

- social media tools (e.g. Twitter, LinkedIn, Facebook, YouTube and Google+)[9]
- cloud sync storage (e.g. Dropbox and Google Drive)
- mobile devices, both parliamentary issued and privately owned (e.g. mobile phones and tablets)
- other personal devices, such as PCs, laptops and encrypted USB memory sticks

With the introduction of Office 365 into the parliamentary workplace, staff are encouraged to use this corporate storage space that facilitates remote access and thus negates the need to make use of other cloud sync storage applications, USB sticks and so forth.

Personal and/or sensitive parliamentary information should not be sent to web-based email accounts, social media tools or taken off or stored away from the Parliamentary Estate without authorisation from your manager or head of office. This includes work-related information which must never be saved to your home computer, laptop or personal USB memory stick.[10]

[9] Staff need to create and manage accurate records of their business activities to ensure decisions and actions can be accounted for. This includes social media activities. When using social media in an official capacity, staff are creating records which provide evidence of business transactions and activity.

[10] Please refer to *Your Role in Safeguarding Information: A Guide for Staff of either House & PICT*.

7.3 Classification

The *Classification Scheme for Parliamentary Records* is a management tool which categorises what information the House administrations create and receive in the course of their business. Broken down according to the business functions, activities and processes undertaken throughout the administrations, the purpose of the *Scheme* is to describe the information landscape across the Houses. It provides the framework for organising information and is a means through which high level policies relating to access, security, retention and disposal can be applied. The process of classifying information can therefore:

- identify information that should be created because of their evidential value to the Houses
- assist in the consistent and logical organisation of information to improve retrieval of that information by staff and their successors
- be used to identify, and to ensure consistency about, how long information should be retained for and what should happen to it at the end of its active life e.g. be destroyed or transferred to the Parliamentary Archives for permanent preservation
- determine security and access levels for different types of information

Classification does not apply to data held in databases or corporate systems that do not lend themselves to classification (e.g. HAIS (HC), MyHR (HL)).

7.4 Maintenance

Digital information systems must contain metadata (i.e. descriptive and technical documentation) that ensure the integrity of the information as a corporate asset, as well as making sure that accessibility and use are sustained for as long as the information is required (which may include migration across systems). Information and records management requirements should be included at the design stage of these systems.

Business recovery plans should take into account the need to protect information which is vital to the continued functioning of each House in the case of disaster or emergency.

7.5 Disposal

Information must be retained only for as long as it is required to support the House administrations in meeting their business requirements and legal obligations, for reference or accountability purposes, or to protect legal and other rights and interests and no longer. At the end of that time, information will either be destroyed by Departments/Offices in line with policy or preserved permanently by the Parliamentary Archives.

Retention and disposal instructions are set out in the *Authorised Records Disposal Practice* (ARDP), the House administrations' policy on the retention, destruction and archiving of its business information. The ARDP covers information regardless of physical location or the format or system in which it is held.

Destruction/deletion of information must be:

- carried out in accordance with instructions in the ARDP only
- carried out in as secure a manner as is necessary for the level of protective markings of the information, so that reconstruction or recovery is unlikely
- documented
- subject to the approval of an authorising officer

Data held in databases and systems (including Data.Parliament) is also subject to a retention period. The individual or group that manages and provides the service the system or database supports has responsibility for working with the IRMS to make sure that purge cycles are reflected in the ARDP and for ensuring that data is destroyed as per policy.

Additionally, in the age of digital publishing, databases and systems may also hold the definitive version of Parliament's e-publications (e.g. Library notes, committee proceedings and evidence). Teams with responsibility for creating and maintaining these publications must ensure this is reflected in the ARDP and work with the Archives to ensure copies of these publications are maintained in Parliament's Digital Preservation System for long term preservation.

Social media is not inherently a type of record; it is another format in which a record can be expressed and should be subject to a retention period. Teams using social media must liaise with the Parliamentary Archives to agree appropriate disposal procedures.[11]

Individuals will be held responsible for ensuring that parliamentary information held on mobile or personal devices (including home PCs and laptops as well as mobile phones, tablets and USB memory sticks and so forth) is destroyed as per policy.

Section 77 of the Freedom of Information Act 2000 makes it an offence for any person to deliberately destroy a record after it has been requested with the intention of preventing its disclosure. Destruction must be delayed until the matter is closed, including ensuring that any complaint and appeal provisions have been exhausted.

The efficient and timely disposal of information is hampered by copying and by sharing it widely via email; the originator may destroy information as per policy, but recipients may still hold it. It is vital that copies are kept to a minimum and that these are destroyed once their business need has passed.

8. Monitoring Compliance

The IRMS develops and implements processes to monitor compliance with this policy, and provides advice and guidance to Departments/Offices where non-conformance is occurring. In cases of a serious violation of the policy or serious risk to the business, this will be reported to the Clerk of the Parliaments or the Clerk of the House as appropriate.

9. Review and Revision

This policy will be reviewed and evaluated in line with changes to business process and compliance requirements no later than 2017.

10.Related Legislation, Standards and Policies

This policy is written in reference to the following pieces of legislation and related standards:

- Freedom of Information Act 2000 and the *Code of Practice on the Management of Records under Section 46 of the Act* (only Part I applies to the Houses of Parliament)

[11] The web archiving programme is the appropriate means to capture most social media sites for permanent preservation. However, the technological limitations mean that this is only possible on a best endeavours basis – the Archives cannot guarantee to have archived particular content. The existence of the web archiving programme needs to be taken into account when considering mitigations for risks around inappropriate content being published.

- Data Protection Act 1998
- Environmental Information Regulations 2004
- ISO 15489 Information and Documentation – Records Management
- BSI DISC BS10008 Code of practice for legal admissibility and evidential weight of information stored on electronic document management systems
- ISO 16175 - Information and documentation. Principles and functional requirements for records in electronic office environments (three parts): ISO 16175-1:2010 Ed 1: Overview and statement of principles; ISO 16175-2:2011 Ed 1: Principles and functional requirements for records in electronic office environments Guidelines and functional requirements for digital records management systems; ISO 16175-3:2010 Ed 1: Information and documentation. Principles and functional requirements for records in electronic office environments. Guidelines and functional requirements for records in business systems

This policy should be read in conjunction with other information, security and data policies, both Parliament-wide and within each House, including:

- House of Lords and House of Commons' Data Protection Policy Statements
- Parliamentary Information Technology Security Policy
- Parliamentary Protective Marking Scheme Guidance
- Procedures for reporting the loss or misuse of information and/or equipment
- Information security guidance for staff of both Houses
- House of Lords Policy on political impartiality and safeguarding official information
- Parliamentary Archives' *Collection & Acquisition Policy*