

Public Service

 **ombudsman**

Information Management Policy

V1.3 July 2026

1 Purpose

- 1.1 Information is central to the work of the Public Services Ombudsman. It provides a full and accurate record of our activities, and informs public scrutiny, research, decision making, and policy development. We are responsible for a large amount of information, which must be managed to ensure good governance, deliver our casework functions effectively, manage risk, and comply with important legal and regulatory obligations.
- 1.2 This policy provides a framework for managing our information and records, covering storage, access, protection, retention and disposal of information. 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 Policy Scope

- 2.1 This policy applies to all recorded information created, received, and maintained as evidence of a decision or an action, or which is an asset held by the Public service Ombudsman in pursuit of legal obligations or the transaction of business.
- 2.2 This includes information relating to core activities responding to complaints as well as that relating to wider supporting activities such as finance, digital services, security, and facilities management. Examples include, but are not limited to:
 - Documents and data (both structured and unstructured) held in digital systems and external web-based collaboration platforms
 - Emails, chats, instant messages, and text messages (including WhatsApp or other messaging applications if used for work communication)
 - Hard copy information and files
 - Inputs and outputs associated with the use of approved AI productivity tools.
- 2.3 Audio and video recordings, photographs, imaging and multimedia content.
 - Building maps and plans
 - Social media (including Facebook posts, tweets etc.)
 - Content related to the development of Ombudsman publications (e.g. drafts prior to publication) and the final digitally published versions

- 2.4 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.

3 Out of Scope

3.1 This policy does not apply to:

- Information processed on internal systems on behalf of another controller, e.g.:
 - Workplace Equality Networks
 - Information and communications created by staff acting in their role within a trade union
- Personal or non-work-related information which pertains solely to an individual's personal affairs held on corporate systems, as per the Acceptable Use Policy
- External materials acquired and kept solely for reference

4 Legal Requirements

4.1 We will comply with all statutory and regulatory requirements relating to the use and management of records. In particular, the following pieces of legislation are key:

- Parliamentary Commissioner Act 1967
- Health Services Commissioners Act 1993
- Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR)
- Freedom of Information Act 2000 (FOIA)
- Environmental Information Regulations 2004
- Human Rights Act 1998

4.2 This list is not exhaustive. The statutory bar on disclosure of information contained in s.11 PCA 1967 and the HSCA 1993 prevents the disclosure of information obtained during or for the purposes of an investigation except in limited circumstances. S.44 FOIA confirms that we are not obliged to disclose that information in response to a FOIA request and s.31 DPA exempts us from the duty to release personal information where doing so would be likely to prejudice the proper discharge of our functions.

5 Who the Policy applies to

- 5.1 Information created as part of carrying out our business is the property of the Public Service Ombudsman and individuals and teams entrusted with its custody are expected to manage it appropriately. This policy therefore applies to all staff, including permanent and temporary staff, and extends to contractors, consultants, secondees and volunteers undertaking work on behalf of us.

6 Specific Roles and Responsibilities

- 6.1 **All staff** (including contractors, consultants and secondees) are required to:
- 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.
- 6.2 **Assistant Directors** 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.
- 6.3 **Assistant Directors** are responsible for the day-to-day assessment and mitigation of risks to the information their team or business area creates and stores. This includes ensuring that this information is adequately secured and protected, shared, reused, and published where appropriate, and that disposal of information is authorised in accordance with the [Retention Schedule](#). These responsibilities apply wherever information is processed and stored and will include Microsoft Teams workspaces and any other corporate systems or applications their business area may use. They provide assurance to the SIRO that risks have been identified and addressed, and that business practices accord with policies and guidance.

- 6.4 **Team information managers** (known as business contacts for Teams workspaces) nominated by Assistant Directors (or by the owner of a collaboration Teams workspace) are a link between business areas and Privacy, Integrity and Assurance and Digital which are responsible for managing information in compliance with this policy and legislative requirements, and the technological solutions for the management of digital information respectively. They help colleagues in their team or business unit adhere to information management policies by providing local guidance, communicating relevant 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 Teams workspaces and use of any associated Office 365 applications as well as other applications their business may use to process and store information.
- 6.5 **The Senior Information Risk Owner (SIRO)** own the information risk at Executive team level and ensures that policies and processes are in place for the effective management of information. The SIROs is supported by a deputy SIRO.
- 6.6 **Privacy, Integrity and Assurance** is responsible for managing corporate information management policies; advising users on compliance with information rights legislation, such as the Data Protection Act 2018, the UK GDPR and the Freedom of Information Act 2000; providing training and guidance, assessing compliance, and supporting Teams business contacts. They are also responsible for increasing awareness of information security risks, developing guidance, and investigating and reporting information losses/personal data breaches where necessary.
- 6.7 **Digital Services** 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.
- 6.8 **The Strategic Information Risk Group (SIRG)** supports Assistant Directors and system owners to manage and mitigate information risks.

7 Policy Requirements

- 7.1 Users must create and keep information which enables the effective delivery of the key functions, or which supports the delivery of these functions. Information must provide full and accurate evidence of communications, decisions made, actions taken, and authorisations given.
- 7.2 Each business areas must establish what information must be created to fully document their activities, considering the operational, legislative and regulatory environment.

- 7.3 We will aim to maintain a single, authoritative source of the truth, which is shared appropriately and reused across different service areas. Users must try to avoid creating or keeping duplicates of information.
- 7.4 Information will be captured and maintained in such a way that it is readily identifiable, accessible and retrievable at all times throughout its lifecycle.
- 7.5 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).
- 7.6 Users must only store digital information on corporately approved systems where it is available to other, authorised users. On occasions where this has not happened, Assistant Directors or their delegated information managers must arrange for information to be transferred into an approved system and erased from elsewhere.
- 7.7 The primary corporate system for unstructured documents and information is a Teams workspace (Teams workspaces utilise SharePoint) or SharePoint document libraries. Personal spaces such as OneDrive must not be used to store the only copy of information, apart from certain line management information or very early drafts. Users must not store information on personal devices, non-Digital issued removable media, or send it to or store it in personal email, cloud storage, or social media accounts.
- 7.8 We do not recognise social media (e.g. Twitter, Facebook), messaging applications (e.g. WhatsApp, Messenger) or free web-based platforms (e.g. Trello, DropBox, Slack) as appropriate systems for storing work related personal data in line with this policy (separate from where they are approved in certain, limited circumstances). As far as possible, the features of Microsoft 365 should be used to replace these services. Regardless of the above any information held on these applications is still covered by the Freedom of Information Act and Data Protection legislation and must be available to be considered for disclosure.
- 7.9 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 and appropriately protected from fire, water ingress, and other hazards.

8 Organisation and Control

- 8.1 We will put in place controls to establish what information it holds and where to be able to understand its value and manage it appropriately.

- 8.2 Business areas must ensure that they understand the information they hold and the appropriate controls that apply.
- 8.3 Business areas must ensure hard copy information is managed appropriately according to its sensitivity. If held in offsite storage it must be appropriately logged by Privacy, Integrity and Assurance.
- 8.4 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 necessary.

9 Access and Sharing

- 9.1 We aim to promote a working culture of openness and collaboration. Information that is not sensitive should 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. See Appendix 1). Sensitive information will be defined and understood by users and managed accordingly for the period that it remains sensitive.
- 9.2 Technology planning must take access permissions and information sharing in systems into account.
- 9.3 Assistant Directors 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. This will usually be achieved by ensuring information created and saved within their business area is stored in the appropriate Teams workspace with up-to-date access permissions (See Appendix 1 for further details).
- 9.4 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.
- 9.5 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. See Retention Schedule
- 9.6 Users must report information losses and breaches of information security to Privacy, Integrity and Assurance as soon as they become known so that they can be investigated and monitored.
- 9.7 Where 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.

10 Evidential Weight

- 10.1 We will put in place controls to ensure that information can be relied upon as authoritative, authentic and having integrity.
- 10.2 Hard-copy information that is scanned with the intention of destroying the original will be scanned to a standard that ensures legal admissibility.
- 10.3 Appropriate version control procedures should be used to ensure that superseded version of information are retained in accordance with the relevant legal requirements, business needs and the Retention schedule.
- 10.4 Audit trails of activities relating to information in digital systems will be created and steps taken to protect them from accidental or malicious access, alteration, or loss.

11 Retention and Disposal

- 11.1 Information will be retained only for as long as it is required to support us in meeting its 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 in certain defined cases be retained 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.
- 11.2 The [Retention Schedule](#) details how long information should be kept for and how information should be disposed of.
- 11.3 Information must be retained and disposed of in a timely fashion, in line with instructions in the Schedule. This includes data in business systems and databases. Where no suitable instruction can be identified, advice must be sought from Privacy, Integrity and Assurance but will ordinarily be two years from last edited or accessed. *The appropriate retention label should be selected if a document needs to be retained for a period other than two years.*
- 11.4 Users must not dispose of information without authorisation from the relevant Assistant Director.
- 11.5 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.
- 11.6 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.

- 11.7 Teams with responsibility for creating and maintaining digital publications must ensure these are included in the Schedule and work to ensure copies of these are transferred for digital preservation.
- 11.8 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 our custody or dispose of it in line with policy and provide confirmation of that disposal upon request.

12 Compliance

- 12.1 Compliance with the areas that are set out in 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 our information. It should also include regular system reporting and audits to monitor security of information and adherence to information policies. Information Governance 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 SIRO.

13 Organisational and Technological Change

- 13.1 Information management issues must be taken into consideration during significant organisational change (whether internal restructures, 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.
- 13.2 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 continue to work with Privacy, Integrity and Assurance to review solutions and ensure that they meet policy requirements and that controls in place are still appropriate.

Version control

Date	Version	Amends	Owner of amends
5 June 2023	0.1	Draft	Alex Daybank
23 June 2023	0.2	Revised Draft	Alex Daybank
19 July 2023	1.0	Approved	Angharad Jackson
14 Nov 2023	1.1	Sensitivity label changes added	Alex Daybank
1 Apri 2025	1.2	Updates to reflect org changes	Alex Daybank
8 July 2026	1.3	Minor updates	Alex Daybank

Appendix 1 – Application of sensitivity labels

1. Sensitivity labels

- 1.1 By default, information must be accessible to anyone across the organisation. This means that standard office documents and emails will receive a *General* classification applied automatically.
- 1.2 Documents with this marking may be shared with anyone and the recipient will be able to read and comment (collaborate access).
- 1.3 Occasionally, documents will contain information of a more sensitive nature, such as staff management information. This information will need to be locked down to a specific audience such as between a line manager and their direct report. To apply appropriate access restrictions, the *Restricted* sensitivity label must be selected. Once this is applied to a document you will be prompted to select the names of the individuals who need access and the type of access (read, change or full control).
- 1.4 In some cases where there are specific requirements to lock documents down to the same group of staff within a business area an additional sensitivity label will be made available. This label must be used in the same way as the *Restricted* label, but the distribution list will be pre-populated. These labels will only be visible to the business areas that require them.
- 1.5 Where a document contains sensitive information, and the use of the *Restricted* label is necessary you should avoid adding any sensitive and/or personal data to its name. This is because whilst the content of the document will be locked down the name of the document will be returned in a search.
- 1.6 If you access a document marked with the *General* marking and think that this is incorrect you should notify the owner of the document in the first instance. If you remain uncertain you should contact Privacy, Integrity and Assurance by submitting a query using HelpHub.
- 1.7 If you think the *Restricted* marking has been incorrectly applied to a document anyone with *full control* can change this. If you have not been given this level of access, you should contact the owner in the first instance and if you remain concerned contact the Privacy, Integrity and Assurance.

- 1.8 The General label will be applied to emails by default, there is no requirement to change this.
- 1.9 If a document with a *Restricted* label is attached to an email you will automatically be prompted to change the email label to *Restricted*. This is in addition to the Egress sensitivity label.