Records Management Strategy 7: Disposal of documents and records

New policy number:	**579**
Old instruction number:	**MAN:A015:a8**
Issue date:	**16 April 2008**
Reviewed as current:	**10 May 2023**
Owner:	**Chief Information Officer (ICO)**
Responsible work team:	**IM Document Management**

Contents

1 Introduction

1.1 This policy explains how to dispose of documents and records.

2 Disposal of records deposited in the records centre

2.1 Procedures are in place for the confidential destruction of documents that are records and that are due to be destroyed once a period of retention has expired.

2.2 All records sent to the ICT Document Management Team (DMT) for deposit with the Records Centre have a retention period assigned to them (see RMS 5). An annual process is carried out by the DMT to identify all records due for review. Reports of records due for review are sent to the depositor and the depositor will either sign off the records for destruction or, if necessary, assign a new review date. Arrangements are in place for the confidential destruction of the records using an external specialist contractor and a destruction certificate is provided (see section 4 below).

2.3 The records centre keeps records of when a record is destroyed and the details of its destruction. The Records Centre database is updated to indicate the destruction, giving the date that the action was carried out. The signed authorities for destruction are also retained.

3 Disposal of records held in SharePoint

3.1 Some procedures are in place for the confidential destruction of electronic records that are due to be destroyed once a period of retention has expired.

3.2 All records in SharePoint have a retention period assigned to them (see RMS 5). The procedure for destruction of records in SharePoint will be determined at a later date when the system is implemented.

3.3 SharePoint will audit the details of destruction giving the date that the action was carried out. The authorities for destruction are also retained.

4 Local destruction of documents as part of normal housekeeping

4.1 Before any local destruction of documents (paper or electronic) takes place, managers must make sure they are aware of any retention periods. The DMT set and maintains standards for retention that reflects legal and other requirements; a copy of the up-to-date retention schedule can be provided on request. Advice about the correct periods for document retention can be provided by DMT.

4.2 When deciding whether destruction as part of normal housekeeping is appropriate, ask yourself whether unique or valuable information will be lost.

4.3 Destruction as part of normal housekeeping should not be used to:

- Destroy records which document the significant operations of a department and may have long-term value;
- 'Weed' papers within files. Papers should not be removed from files unless allowed by a specific disposal authority. Such action can destroy the integrity of the files as one piece of paper may have little value, but collectively the papers may present a complete picture of the activity documented; and,
- Destroy business-related e-mail before it becomes part of the formal record. Key emails documenting business processes should be moved into formal document management systems in SharePoint.

4.4 Destruction as a 'normal administrative practice' or housekeeping can take place where documents are duplicated, unimportant or for short-term use only (and this applies to both paper and electronic records). This regular day-to-day process is not intended to replace the deposit of non-active records with the records centre or disposal arrangements for records in the Record Centre.

4.5 The following records may be destroyed locally as part of normal housekeeping practice:

- superseded manuals or policies (except for a master set which includes the superseded portions);
- library material (except for assets requiring writing off);
- catalogues and trade journals;
- information copies of press cuttings, press statements or publicity material;
- letters of appreciation or sympathy, or anonymous letters;
- requests for copies of maps, plans, charts, advertising material or other stock information;
- address lists and change of address notices;
- calendars, office diaries and appointment books;
- facsimiles, where a photocopy has been made for file;
- rough drafts of reports, correspondence, routine or rough calculations;
- routine statistical and progress reports compiled and duplicated in other reports;
- abstracts or copies of formal financial records maintained for convenient reference; and
- telephone messages.

5 Disposal and information security

5.1 Once a local decision to destroy a document has been taken it should be disposed of in an appropriate manner. A decision should be made whether the record is sensitive or whether the document(s) contain personal information. Personal information, in particular, should be disposed of in a secure way to ensure compliance with the Data Protection Law.

- If the record is not sensitive it can be placed in the recycling bins.
- If the records are sensitive, sacks are available on POMS or HQ staff can obtain them from the Document Management Team. Sensitive records from non HQ offices will be collected by the Procurement Department van service. HQ staff should bring filled sacks to the mail room. For larger quantities (20 sacks or more) direct collections by our confidential waste contractor can also be ordered on POMS.
- The Union Street dry hubs are fitted with secure sensitive waste containers. These replace the use of sacks for HQ staff although sacks are available for larger quantities.
- The use of shredders will be restricted to information where the security classification level requires it to be shredded on site.

5.2 Where documents are security marked (under any security classifications system), special arrangements may apply to destruction.

Document history

Assessments

An equality, sustainability or health, safety and welfare impact assessment and/or a risk assessment was last completed on:

EIA	04/07/08	SDIA	18/05/23	HSWIA	12/05/23	RA	

Audit trail

Listed below is a brief audit trail, detailing amendments made to this policy/procedure.

Page/para nos.	Brief description of change	Date
Throughout	Policy reviewed as current. Reference to the EDRMS system has been removed from section 3.	20/05/2011
Throughout	Minor amendments have been made to the wording throughout this policy please read to familiarise yourself with the content.	29/05/2014
Throughout Page 4	Minor changes to wording throughout, including wording of title. 'Subjects list' table - template updated.	19/01/2015
Throughout	Minor amendments throughout.	05/06/2017
Page 2	A warning heading has been added to this policy.	12/07/2021
Page 2 Throughout	Warning removed. Reviewed as current with minor amendments made throughout.	10/05/2023
Page 4	SDIA updated.	19/05/2023

Subject list

You can find this policy under the following subjects.

Records management	

Freedom of Information Act exemptions

This policy/procedure has been securely marked due to:

Considered by: (responsible work team)	**FOIA exemption**	**Security marking classification**