Records Management Policy

This is version 2.2 of the policy and was updated on 3 February 2015. This policy replaces: DWP Benefits Document and Data Retention Guide; Corporate Memory Guide; Electronic Storage Policy and Retention policy for Datasets (DWP Data Retention Policy for Analytical, Research, Business Management Data and Financial Records).

Contents

1. Introduction

The Records Management Policy tells you which documents and data you need to keep, for how long and where to keep them. The Policy will be reviewed annually by the policy owner (Knowledge and Information Management Division) in consultation with stakeholders.

1.1 What documents and data are covered by this policy?

This policy sets retention periods for all documents, data and records created by DWP staff however they are created or stored.

This policy is format neutral, which means that it includes paper documents, electronic records, emails, social media posts, databases, websites and Intranet sites, etc.

DWP has two types of record:

- Corporate records – this includes all documents and data created by you in day-to-day business. **All** 'significant' corporate records created by or on behalf of DWP are **public records** and must be treated as such. These public records may eventually be viewed by members of the public at The National Archives
- Benefit records – this includes all claimant or customer-related documents and data. These are not public records.

1.2 Why does the Department have a Records Management Policy?

The Department is legally required to create and manage corporate and benefit records to provide an audit trail of the organisation's decision-making process and activities.

This policy ensures that DWP complies with document retention requirements:

- The Data Protection Act states that data should be kept as long as there is a business need for it and for no longer than appropriate.
- The government's Information Principles state that information should be effectively managed from creation to destruction.
- Corporate records are kept to comply with the Public Records Act.

This policy is designed to ensure that DWP retains only those documents and data which support business objectives; saves money and space by reducing information storage costs; protects against allegations of selective document destruction; manages our information risks; and avoids destroying documents that need to be retained.

Failure to retain documents and data, and to destroy them at the right time, could result in serious consequences, including:

- Fines from the Information Commissioner
- Lack of evidence for court cases
- Benefits paid incorrectly
- Damage to DWP's reputation
- Personal data not destroyed in line with Data Protection Act requirements
- DWP may be unable to answer Freedom of Information (FoI) requests or deal with complaints received if documents are destroyed at the wrong time

Each record (i.e. document, data or piece of Departmental information) must be evaluated to determine how it should kept and for how long. You must only retain a record for as long as there is a valid business or legal requirement to keep it. Teams should regularly review the information they hold to ensure it remains appropriate, up-to-date and necessary for the effective management of the

business. See the Appendices for details of the legal and business requirements for document retention.

2. Retention principles of corporate records (documents and data)

2.1 General principles

You must keep records of the decisions you make, the advice you give, anything you do in the course of your work if it is significant.

All 'significant' corporate records must be printed to paper. Any electronic document, including emails and Intranet documents, must be printed to paper and put in a Registered File or Corporate Record Box as soon as it has been identified as a 'significant' record. This is to ensure that DWP meets its legal obligations under the Public Records Act (PRA). Currently, we do not have an Electronic Document and Record Management System in place to meet PRA obligations.

See the Registered Filing Guidance for details of how to set up and manage Registered Files and Corporate Record Boxes.

There is an element of judgement in deciding what you consider 'significant'. See the Appendices for details of the legal and business requirements for document retention, there is an index to the Appendices in section 7.

The following gives a brief summary of the minimum requirements for significant corporate records:

SAVE: information relevant to Departmental business such as:

- Documents that have a business need to be retained
- Research which is published and unpublished
- Advice and briefing for Ministerial decisions
- Delivery of Ministerial responsibilities to Parliament
- Ministerial correspondence
- Development of policy and guidance
- Substantial contributions to policy and legislation
- Background on externally published online or hard copy guidance and procedural documents
- Records of measures taken to comply with legal obligations
- Documentation of significant programmes and projects
- Contracts, tenders and payment records
- Information required for audit purposes
- Drafting of legislation

DELETE: duplicates documents and documents such as:

- Policies you may have contributed to but are not the owner of.
- What can be downloaded from an Intranet page – the page owner will keep a copy on the registered file (if applicable).
- Anything available on a Shared Area which has already been printed and placed in Registered Files or does not have a current business need.
- Records of meetings not directly impacting Departmental business.
- Arrangements for meetings, e.g. room bookings, meeting invites, etc.
- Routine correspondence with internal service providers.

- Documents received ‘for info’ where you have no direct responsibility.

2.2 Where should corporate records be stored?

Documents must only be held electronically if they relate to current Departmental business or the activity of an individual member of staff. Departmental file naming and version control conventions should be used.

If documents do not meet these criteria, they should be deleted and if applicable the ‘print to paper’ policy followed. See the Appendices for details of where documents should be stored.

DWP currently has a ‘print to paper’ policy because, in general, our existing IT systems do not provide sufficient certainty about what documents or versions were agreed or communicated at a given time. We have to keep to a print to paper policy for corporate records as there is no ability in DWP to archive electronic records in compliance with records management legislation.

Documents that are classed as significant records must be kept in:

- **Registered Files –** this is the formal paper-based system used by DWP to control and manage its significant corporate records, which include those considered significant in terms of public interest, spending or have a potential national impact.
- **Corporate Record Boxes** – these are used for bulky records (e.g. finance, legal, estates and procurement documents) or records that don’t need to be kept for 15 years.

Documents that are not classed as significant may be stored in the team’s Shared Drive, personal storage (MyDocuments) or Outlook. Personal storage must only be used for your personal documents and information relating to a member(s) of staff that you manage.

2.3 Destruction of corporate records

Records, documents and data should be destroyed according to the business/legal requirements as detailed in Appendices of this document.

Documents identified as ‘significant’ records, must **not be** destroyed locally. They must be placed in a Registered File or Corporate Record Box and sent to Heywood Stores where they will be reviewed as appropriate.

For further information: see related guidance on the use of government security classifications in DWP.

See also desk aids on corporate records, file naming and version control conventions and destruction of data or contact the KI&RM Team.

3. Retention principles of benefit records (documents and data)

3.1 General principles

The retention periods for benefit records (and customer/claimant records) are based on the business need to keep that information, i.e. maximum late claim and appeal time limits (13 months and 14 days) as specified in the benefits legislation. Having retention rules meets the requirements of the Data Protection Act (DPA). Retention periods apply to all benefit documents and data whether the claim is successful and not.

3.1.1 Classification of documents

You must examine **all** documents and data relating to a case as you action them, then classify them under one of the following categories **Supporting** documents/data, or **Ephemeral** documents/data:

- **Supporting** documents/data are those which support an outcome decision and contain information on which a decision has been based, e.g. claim and review forms, and/or determine the amount of payment, e.g. copies of current wage slips. Documents/data required for security and accuracy checks are also classified as supporting.
- Any documents/data that do not fulfill the criteria for supporting are classified as **ephemeral**, and should be destroyed after 4 weeks, unless marked or identified as exceptions. Ephemeral documents used for checks should be reclassified as supporting.

Documents and data that **support** the benefit decision are retained for 14 months after the case is closed, unless an alternative retention period is given in the retention periods for benefit records section.

Retention periods of supporting documents/data only begin once entitlement ends AND all action has been completed. If payment or entitlement continues, the case remains LIVE and documents or data must not be weeded/destroyed. The retention period of ephemeral documents begins at date received. See deskaid on retention periods for supporting benefit documents for definitions of Put Away (PA)/Dormant/case closure. See DRS guidance for details.

The **Document Repository System** (DRS) has two additional classifications for electronic images:

- **Untraceable** which allows missing information for example NINO, to be added to the electronic image so it can be linked to an individual claim/case. Document classification is then changed to supporting/ephemeral as appropriate. If the electronic image is not traced it is deleted after 6 weeks.
- **Expunge Immediately** which is for items that have been scanned in error, these images are deleted within 72 hours. See DRS guidance for details.

3.1.2 Exceptions to retention periods of benefit records

There are **exceptions** to these retention periods, e.g. if there is fraud, overpayment, appeal or a complaint – see Appendix A for the full list of exceptions.

When an exception applies, documents and data will not be destroyed until all exceptions have been lifted/cleared, the normal retention periods will then apply.

3.1.3 Benefit records in other formats

Benefit records are also kept in other formats; these must follow the current document and data retention policy, including additional retention periods for exception cases and be classified as either ’supporting‘ or ’ephemeral‘.

a) **Scanned images** of benefit records must:

- Meet ‘legal admissibility’ guidance once scanned, in line with British Standard BSI PD0008:2008.
- Original documents must be destroyed 4 weeks following scanning, unless identified as a ‘valuable’.

b) **X-rays** should be scanned into DRS or equivalent and **should not** be kept on CD/DVDs or sent to Heywood Stores for storage. Businesses must store them correctly to ensure that the x-rays are readable for the whole retention period. Prior to X-rays being held on CD/DVD they were held on X-ray plates, these can be retained in Heywood Stores in a Card X-ray pouch.

c) **Recorded telephone conversations** must:

- Meet 'legal admissibility' guidance, in line with British Standard BSI PD0008:2008
- Be destroyed if a customer signs and returns a claim form - the claim form becomes the supporting evidence.

- **Note:** With **Customer Account Management** (CAM), the telephone conversation is recorded as a replacement for signed documentation. The recorded telephone conversation must not be destroyed until the retention period for all the benefits the call refers to have elapsed. CAM telephone calls are retrieved from the Verint telephony system.

3.2 Where should benefit records be stored?

Hardcopy (paper) benefit records should be stored as follows:

- Supporting records must be sent to remotes stores via FARIO.
- Ephemeral records must be stored locally

Electronic benefit records are stored on DRS, Verint, CAMLite etc. Data is stored on legacy benefit systems (e.g. JSAPS, WFPS, PSCS etc.) They are stored for the same retention periods as the hardcopy (paper) supporting and ephemeral documents.

Digital media, such as CDs/DVDs, and encrypted memory sticks are only allowed for storage of personal data in agreed instances, e.g. x-rays or fraud evidence. Businesses that store data on CD/DVD must ensure that it is stored correctly and that the data is readable throughout the retention period, which may require migrating the data to new formats to maintain data integrity/readability, as well as when IT changes. This digital media **must not** be sent to remote stores; it should be stored and destroyed locally following security guidelines. Please contact the KI&RM Team for advice.

3.3 Destruction of benefit records

Benefit records must be destroyed as follows are:

- Supporting records **must not be** destroyed locally. Once a case is closed, FARIO teams **must** be informed, as they **must** enter a case closure date in FARIO. This will trigger document destruction at the correct time for benefit records held in remote stores.
- Ephemeral records should be destroyed locally.

Benefit records should be destroyed according to the business/legal requirements as detailed in Appendix A of this policy.

When destroying benefit documents/data we are applying DWP Records Management Policy (RMP) and **not** the Data Protection Act (DPA) as the DPA does not specify retention periods.

Standard responses should be used when members of the public make enquiries about the destruction of records:

- Where documents/data **have been destroyed in line with the RMP**, use Letter 1.
- Where documents/data **have not been destroyed in line with the RMP** and may have been destroyed in error (either partially or fully) use Letter 2.

Data Protection Officers should also refer to the Subject Access Request (SAR) Guide – a definition of when a benefit record is 'held' for SAR requests is given in section 4.1.

If a benefit record is destroyed, details must be kept of when it was destroyed. This record is held on FARIO for records held in remote stores.

See also section on: exceptions and retention of benefit records.

For further information: Desk aids on retention of benefit records or contact the KI&RM Team.

4. When is a document 'held' or 'not held' for FoI purposes?

Although all requests for information made under the Freedom of Information Act 2000 (FoI) will need to be considered on a case by case basis, this section sets out the general DWP policy on when information will be 'held' or 'not held' for FoI purposes.

DWP will also apply the same principles for determining whether information is 'held' or 'not held' in relation to external enquiries falling outside the FoI and for subject access requests (SAR) made under the Data Protection Act 1998.

Documents and information are classed as 'held' or 'not held' if they meet the following criteria:

4.1 Held

- Registered files, Corporate Record Boxes and benefit records (for SAR requests) are classed as **held** until the files are marked as 'Selected for destruction' on the FARIO file management system. Note: DWP does not currently have any electronic corporate records, therefore all 'significant' records must be printed to paper, see section 2.1 for details.
- Paper or hard copy documents are classed as **held** until the document is physically transferred to waste recycling or confidential waste bin.
- Electronic documents are classed as **held** if they:
  - are on the current version of Shared Drives or can be retrieved from the 'recycle bin';
  - can be retrieved from the 'recycle bin' for MyDocuments (personal storage); or
  - can be retrieved from the Deleted Items folder or using the 'recover deleted items' facility in Outlook.
- Electronic datasets are classed as **held** until the data is deleted from the database and recycle bin.

4.2 Not held

- Documents held solely on backup tape/drives are classed as **not held** for the purposes of the FoI Act.

For further information: the Information Commissioner's Office (ICO) website for lines to take on deletion of electronic information web and ICO guide on destruction of requested information web or contact the KI&RM Team.

5. Assurance / compliance

The DWP Senior Information Risk Owner (SIRO) owns the Department's information risk policy and risk assessment process. They are responsible for information risk, influencing the board in managing these risk properly, fostering a culture that values, protects and uses the Department's information and knowledge resource for the public good, and maintains a system of control which safeguards the security of information assets and data systems. DWP has introduced a network of Business SIROs to support the DWP SIRO in discharging their accountabilities by taking the lead on their business's strategic approach to managing information risks. Information Asset Co-ordinators (IACs) provide appropriate support activities to enable the Business SIRO to effectively discharge their responsibilities. Information Asset Managers (IAMs) support Senior Responsible Owners (SROs) in meeting their responsibilities for ensuring that risks to information systems and assets have been identified and mitigated with appropriate and effective controls. Nominated contacts and Registry contacts are also in place although these are not Cabinet Office mandated roles.

Compliance with the policy is the responsibility of all staff. Compliance is monitored by Records Storage Strategy Group. Additional compliance forums report into the Records Storage Strategy Group.

Where non-compliance is identified, line managers should be informed and it should be reported to the relevant Business SIRO. Consistent non-compliance should be reported to the DWP SIRO and the KI&RM policies team. It is the responsibility of the Business SIRO and line manager to ensure that corrective action is taken.

There is an annual information audit carried out by the KI&RM team that looks at what records are maintained in each business area. Assurances around the effective management of information assets and their subsequent risks are also obtained as part of the Business SIRO through year reporting process overseen by the DWP Information Security & Assurance Team.

In turn, the Information Security and Assurance Team reports to and is accountable to the Information Management and Assurance Board (IMAB).

5.1 DWP Senior Information Risk Owner

The DWP SIRO is a member of the Department's Executive Team (ET) and provides assurance to the Accounting Officer that the Department's information risks are understood and managed or mitigated effectively. He is supported by a network of Business SIROs.

5.2 Business Senior Information Risk Owners

Business SIROs are in place across the main areas of the Department and are aligned with subdivisions of the business that make sense to an outside observer i.e. the management of the assets looks like the management of the business owning the assets. Business SIROs are responsible for taking the lead on their business's strategic approach to managing information risks, including leading and fostering a culture that values, uses and protect information for the public good, and supporting the achievement of DWP's information management, security and assurance objectives.

Business SIROs are expected to have a good understanding what information is held in their areas and take the lead in the effective management of information risks through the maintenance of a business specific information risk register and Information Asset Inventory.

5.3 Information Asset Co-ordinators

Business SIROs are supported by IACs who proactively engage with them and the SROs to support them in identifying the information risks to their individual assets, exploring if these are being effectively managed and mitigated and providing effective challenge.

5.4 Senior Responsible Owners

In a project/programme environment a SRO has overall accountability for delivery, including management of project and delivery risks. They are responsible for ensuring control mechanisms are designed that safeguard the information assets created by, or used, once the change has been delivered. They will be assisted by the programme/project staff in the management of the information assets.

In the live environment the SRO is the owner of a system or service. They are ultimately responsible, within the first line of defense (directorate and line management level), for ensuring that the system, service and its processes maintain adequate levels of information security, that internal controls exists, mandatory controls are complied with and that they operate effectively. In a live environment, the SRO will be assisted by the IAM and other advisors.

5.5 Information Asset Managers

The main purpose of the IAM is to support the Senior Responsible Owner in meeting their accountabilities for ensuring risks have been identified and mitigated with appropriate and effective controls. The IAM role is a ‘doing’ role.

5.6 Nominated contacts

Each Deputy Director has a nominated contact. Their responsibility is to:

- Ensure the Knowledge Information & Records Management (KI&RM) team has a record of the nominated contact.
- Ensure that benefit and corporate records are being kept and managed within their division (as applicable to business area).
- Provide assurance that Registered Files are set up and maintained.
- Ensure benefit record final action is completed in FARIO, so that retention periods are updated (if applicable to business area).
- Ensure their business unit is adhering to all information management policies.
- Ensure policy colleagues contribute to decisions to open a file when The National Archives has received an FoI request for access to a closed file (if applicable to business area).
- Arrange training sessions or inductions on records management and Registered Files for their division. If required, the training will be provided by the KI&RM team.
- Answer questions from within their division regarding business and corporate records - these queries can be forwarded to the KI&RM Team if required.
- Be a stakeholder for Records Management Policy changes.
- To circulate communications issued by the KI&RM team to their division.

5.7 Registry contact

The Registry contact has overall responsibility for the management of their Registered Files and/or Corporate Record Boxes. This includes:

- Notifying the Knowledge Information & Records Management (KI&RM) team of any changes within their team, such as type of work undertaken by the team, start or end of projects, change of contact etc;
- Produce and maintain an excel spreadsheet containing the details of the registered files created within their area. This must be sent to the KIRM team annually or when requested.

5.8 All staff

All staff have a responsibility to keep records of the decisions they make, the advice they give, anything they do in the course of their work if it is significant.

See also section on: Registered Filing Guidance.

For further information: see our FAQs and Desk aids on retention of benefit and corporate records or contact the KI&RM Team.

6. Contact information

For enquiries on how to keep Registered Files and Corporate Record Boxes or for any other queries, please contact the Knowledge Information & Records Management (KI&RM) team.

For further information: see our FAQs and Desk aids on retention of benefit and corporate records or contact the KI&RM Team.

7. Where should different documents and data be stored and for how long?

Index for the Appendices

Documents and data have different business and legal requirements for their retention depending on the type of document/data.

The appendices provide the retention periods for the following documents and data which are used within DWP; they also give details of where documents should be stored and by whom:

A

- Annual report
- Accounts
- Agenda

B

- Bank account records / statements
- Benefit fraud documents
- Benefit records
- Briefings
- Budgets (team / divisional and

L

- Ledger records
- Legal advice (i.e. to support policy making)
- Legislation
- Legislation-related correspondence
- Letters
- Litigation (including Judicial Reviews)

departmental)
- Business planning

C
- Child maintenance records
- Communications documents (newsletters, notices and questionnaires etc.)
- Complaints document (non-delivery areas)
- Consent forms
- Consultation papers
- Corporate Policy
- Correspondence

D
- Data sets
- Data sets – background information
- Debt Management
- Decision Making and Appeals (DMA)
- Diaries & calendars (Ministerial)
- Diaries & calendars (Non Ministerial)
- DWP Corporate Archive

E
- Emails – organisational, policy-related or claimant/customer related
- Environmental Impact Regulations (correspondance)
- European Social Fund (ESF)
- Expenditure records

F
- Finance documents
- FOI records
- Form (external)

G
- Guidance (external)
- Guidance (internal)

H
- Health and Safety documents
- Human resources documents

M
- Medical Advice (Medical Services Advice Submissions)
- Meeting correspondence
- Ministerial correspondence
- Minutes
- Mission statement

N
- Newsletter or Internal communication/publicity

O
- Organisation chart
- Organisation-related correspondence

P
- Parliamentary documents
- Parliamentary Questions
- Policy documents
- Policy–related correspondence
- Presentations
- Press release
- Proceedings
- Procurement - involving Deeds
- Procurement - over £5000
- Procurement - short term retention
- Procurement - under £5000
- Programmes (conferences etc.)
- Project document - major project
- Project document - minor project
- Promotional materials (external)
- Prosecutions
- Public notice
- Publications - external (including leaflets, research and forms)
- Purchases

Q
- Questionnaires

R
- Receipts & revenue records
- Reports

I

- Information from working with Ministers and other senior officials (see: Submissions & Briefings)
- Internal form (templates)
- Internet pages
- Intranet text
- Invoices
- IT forms

S

- Salary records
- Service level agreement (SLA)
- Social Media posts (including Yammer)
- Speeches
- Subject Access Requests
- Submissions

T

- Terms of reference

Appendix A: Retention of benefit records

All benefit records are retained for 14 months after case closure if they are supporting documents or 4 weeks from date received if ephemeral; unless a non-standard retention period is given in the table below.

The retention periods apply to all claim documents and data whether the claim is successful or not. **They also apply to the benefit processing IT systems.**

Retention periods start from date the case is closed, unless an alternative retention start date is given in the desk aid on retention periods for supporting benefit documents.

There are exceptions to the retention period for benefit records, e.g. fraud, overpayments, appeals or complaints. Files are not destroyed while the exception is in place, once the exception is cleared normal retention periods apply. Identify claims/cases which are exceptions and note them as '**Not for destruction until exception(s) cleared**'.

Temporary embargoes are sometimes placed on the destruction of some benefit records. Note: ALL embargoes MUST be discussed and agreed with KI&RM Team before implementation.

Table showing standard retention periods

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Benefit records **Child maintenance records** **Debt Management records** (including Compensatio	All documents and data, including emails	Standard retention periods for Supporting documents are 14 months after the case ends and exceptions	**DWP guidance** Emailing customers policy **Legal requirements:** Retention is	Data is stored on DWP legacy benefit systems (e.g. JSAPS, DRS, Verint etc.).	DWP legacy benefit systems have data retention periods are built into them.

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
n Recovery Unit & Fraud and ApPen Overpayment documents)		are cleared. See below for non-standard retention periods. Ephemeral documents are retained for 4 weeks from date received.	based on the appeal and late claim regulations under benefit legislation.	Paper documents are stored at Remote Stores	FARIO teams manage the sending, retrieval and destruction dates of paper documents are held in Remote Stores. [**Note:** If you do not update FARIO the records may never be destroyed. You must inform the FARIO team when a case closes.]
Decision Making and Appeals (DMA)	Mandatory reconsideration & appeals process documents and data				
Medical Advice (Medical Services Advice Submissions)	All documents and data, including emails				
Benefit fraud documents	All documents as listed in Retention of evidence files in England and Wales	14 calendar months from the date an evidence file is marked put away (PA) and exceptions under Proceeds of Crime Act 2002 are cleared	**DWP guidance:** Fraud retention of documents guidance. Fraud tapes and digital discs Fraud retention of documents guidance (FRAIMS)	Hard copy of original forms retained at Remote Stores	Fraud teams
	Tapes and	Retain as		Tapes and	

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
	digital discs (including Audio/video tapes and compact / digital versatile discs (CDs / DVDs)	per other Fraud documents. Surveillance tapes / discs that must be kept for 3 years	**Legal requirements:** Criminal Procedure and Investigations Act (CPIA) 1996 Code of Practice (COP) 5.9 Home Office Regulation of Investigatory Powers Act (RIPA) 2000 Code of Practice	digital discs are retained locally	
	All documents as listed in the Fraud retention of documents guidance (FRAIMS)	5 years		FRAIMS	
Subject Access Request (SAR)		3 months	**DWP guidance:** SAR guide	Shared Drive	SAR responder

Table showing non-standard retention periods

Note: the standard retention periods apply if the benefit is not listed in this table, see details above.

Retention of…	Specific documents (if applicable)	Retention period	Business justification for retention period
Carer's Allowance		26 months after PA	Temporary extension to retention period to November 2015.
Debt management	Electronically held customer correspondence (Primary E-Post)	Retain at a customer level, not an individual level, i.e. 14 months after the zero balance has been reached.	Destruction is at customer level, as correspondence includes reference to all outstanding debts.

Retention of…	Specific documents (if applicable)	Retention period	Business justification for retention period
Employment and Support Allowance	ESA55 referral files for live claims **Embargo on destruction of IB55 & ES55s** - awaiting judgment from the Upper Tribunal	72 months (but do not destroy any documents at present - pending an Upper Tribunal judgment)	This is to ensure that the last two Work Capability Assessments are retained
European Social Fund (ESF) Note: for ESF research & evaluation see guidance for research reports.	Documents as listed in Annex A of the ESF guidance.	Retained until 31st December 2022	European Commission (EC) audit and regulatory requirements
	Documents as listed in Annex A of the ESF (Wales) guidance.	Retained until 31st December 2024	
European Refugee Fund Claims (for JSA, ESA & IS claims)	Clerical Claim forms along with relevant evidence supporting claims made by Gateway Protection Programme refugees.	5 years following the closure of the claim/PA.	This is a UKBA (Home Office) requirement to meet EU audit requirements.
Flexible Support Fund	For advisor-related payments	18 months following the financial year in which the application was made or any overpayment was fully recovered/ written off, whichever is the later. RM retention periods apply to FSF payments, see appendix F for details.	Treasury/National Audit Office requirement.
	For FSF Grant funding awards to organisations.	Minimum of 10 years, from date of last payment.	EU regulation requires FSF “to keep records of all de minimis aid paid for ten years from the last payment.”

Retention of…	Specific documents (if applicable)	Retention period	Business justification for retention period
			Page 12 of BIS State Aid Guide
Incapacity Benefit	IB55 referral files for live claims **Embargo on destruction of IB55 & ES55s** - awaiting judgment from the Upper Tribunal	120 months (but do not destroy any documents at present - pending an Upper Tribunal judgment)	This is to ensure that the last two Personal Capability Assessments on form IB85 are retained
Independent Case Examiner (ICE) cases	For data recorded on Respond.	3 years after ICE case closure.	Retaining electronic data for 3 years allows sufficient time for a complainant to consider the outcome of ICE examination of their complaint and exercise their right to approach the relevant Parliamentary Ombudsman.
Industrial Injuries Scheme Benefit Industrial Injuries Scheme Benefit (Except Industrial Death Benefit (IDB)	**Embargo on IIDB miners' files** - see the IIDB guidance for further details.	**For non-miner claims/cases:** 14 months after the date of death or the date of the last decision (PA) whichever is the later. **Do not destroy Miners' IIDB files**	There is an embargo on the destruction of Miners' IIDB files until the coal miners' litigation against the Department of Energy and Climate Change (DECC), as inheritor of the liabilities of the former British Coal Corporation, is complete.

Retention of…	Specific documents (if applicable)	Retention period	Business justification for retention period
Jobseeker's Allowance (JSA)	Labour Market Units (LMU)	Retain on site for 1 month after the last date of the claim. LMUs are to be retained for 14 months after the last date of the claim if they contain: • documents supporting a decision to disallow entitlement or apply a sanction. Or • a fraud, appeal or overpayment marker; or • selected by Performance Management for checks. See the LMU guidance for details of how to process these documents	LMUs are classed as ephemeral from end of claim.
	JSA claimant commitment	Paper copies should be stored in the LMU and follow LMU retention period above. Retain the last electronic version of the JSA Claimant Commitment in each claim in the secured shared folder for 30 weeks after the	Required for rapid reclaim

Retention of…	Specific documents (if applicable)	Retention period	Business justification for retention period
		last date of the claim	
	SL2s	Where there is European Social Fund (ESF) and Match funded provision – Retain until 31/12/2022.	ESF retention guidance.
		Where there is no ESF and Match funded provision, retain for 18 months from referral.	The longest period for contracted provision was 12 months. Also must leave extra 6 months to administer any claims from providers and potential audit.
Main file prints, full record prints, copy records		See deskaid on Main File Prints for details	
Management checks		See deskaid on management checks for details	
MAPPA J forms		Should be retained locally for the period that the restrictions apply. When the restrictions no longer apply the MAPPA forms should be destroyed immediately, in the same way as any other sensitive information.	Required to identify which offenders are MAPPA eligible and the related risk management. See MAPPA guidance for further details.

Retention of…	Specific documents (if applicable)	Retention period	Business justification for retention period
New Enterprise Allowance	All documents relating to NEA financial support	Retain for 18 months after final NEA payment or date of last NEA engagement.	DWP Finance Managers Guide - retention of documents deskaid
NINO Allocation	Successful NINO applications - form CA5400. **Note**: see the Secure NINO Allocation Process (SNAP) Guide	3 years from the date of creation.	3 years is required prevent Fraud or identity theft, and to prevent re-applications and to allow cross reference.
PIP	All supporting documents	24 months from claim closure (PA).	PIP linking rules
Special Payments	All documents relating to Special Payments	**Payments**: Follow the retention periods for payment documents as given in appendix F **Payment refusals** – retain as per the Special Payments Guide.	DWP Financial Redress for Maladministration
State Pension Deferred Lump Sum Payments	The completed DL66 & DL67 and any evidence to support subsequent changes to this decision.	72 months (6 years) after the financial year the payment is made	HMRC, The National Archives (TNA) and National Audit Office (NAO) requirements
Suicide and self-harm documents	All documents relating to suicide and self-harm.	Retain for 6 years following the date on which the incident occurred or the declaration of intention was made.	Health and Safety document retention schedule and customer's suicide and self-harm policy guidance

Exceptions to the retention period of benefit records

The most common exception cases are shown in the following table – once the exception has been cleared normal retention periods will apply:

Type of exception:

- Fraud
- **Overpayments** including: civil proceedings & Recovery from Estates
- **Debt Management** including: Compensation Recovery
- **Appeals** including: Mandatory Reconsiderations
- **Customer feedback or complaints** including: Independent Case Examiner (ICE) cases & Parliamentary Health and Service Ombudsman (PHSO) Cases
- Criminal Cases Review Commission cases
- Cases subject to a **Performance Measurement** check
- **Maxwell Cases** and other pension scheme cessation cases.

When you identify a case as an exception, you **must:**

- Mark the case file and any appropriate sub-files as '**Not for destruction until exception(s) cleared**'
- Set any system indicator
- Note all relevant non-paper data sets and data bases etc. and
- Inform the FARIO team that an exception applies to this claim file.

The exception marking on case file, either paper or electronic, should be removed when any of following apply:

- All action is complete
- The specialist area no longer has an interest in the claim/case
- The file no longer supports a current decision or a decision made in the previous 14 months

The file should be destroyed 14-months (or non-standard retention period as given above) after removing all the exception markers, unless the case remains live.

You **must** inform the FARIO team when an exception is cleared, so that they can set a destruction date.

See also section on: Retention principles of benefit records (documents and data)

For further information: see the deskaids on benefit records or contact the KI&RM Team.

Appendix B: Retention of communications documents

Retention periods start from the date when the document is created

Retention of…	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Newsletter - internal publicity **Questionnaires**	12 months		Shared Drives	Document creator
Internet pages	Until uploaded onto Internet	**DWP guidance:** Internet Archiving Policy Contact the Digital Publishing Team for full details.	The National Archives (TNA) digital continuity plan captures all Internet pages.	Document owner
Intranet text	Until uploaded onto Intranet **Note**. Original policy/ guidance documents must be kept in a Registered File		Shared drive	Document owner

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered Filing Guidance for details.

Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix C: Retention of correspondence

This covers all correspondence received/sent by non-delivery areas; correspondence relating to delivery areas should follow guidance for benefit records.

Retention periods start from the date when the document is created.

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Briefings	Briefings (Internal)	12 months		Shared Drive	Policy team
	Director General briefings for visits, staff meetings and events	12 months			
	Ministerial Briefing / factsheets - including background	20 years	**The National Archives (TNA) & legal requirements:** TNA Guidance on the Management of Private Office Papers; Public Records Act	Registered File	Policy team
Complaints document (non delivery areas)	All papers relating to the complaint	14 months If Registered File required – retention period is 20 years		Shared Drive or Registered File if required.	Letter recipient
Legislation-related correspondence	Environ-mental Impact Regulations (EIR)	2 years after last action on the case	**The National Archives (TNA) requirements:** TNA Retention Scheduling 9: Information	Shared Drive	EIR responder

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
			Management Record		
	Freedom of Information (FoI) – ICO cases	2 years	**DWP guidance:** FoI records retention guidance **TNA requirements:** TNA Retention Scheduling 9: Information Management Record	Shared Drive	FoI responder
	FoI - routine response	1 year			
	FoI – database	5 years		FoI VTR	Central FoI team
	Legal Advice	20 years	**TNA & legal requirements:** TNA Operational Selection Policy Osp42 - Records Of Departmental Legal Branches Public Records Act	Registered File or Corporate Record Box.	Policy team
Ministerial correspondence		12 months		COMET	Ministerial Correspondence Team
Organisation related correspondence	Email exchanges with non DWP stakeholders - ephemeral	4 weeks		Outlook	First recipient if incoming or sending if outgoing emails
	Emails – personal,				

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
	trivial or ephemeral				
	Yammer posts	4 weeks		Yammer	DWP IT
	Social media posts (external)	4 weeks		Social Media e.g. Facebook/ Twitter	DWP IT
	External letters: Received & Replies (non-delivery areas)	12 months		Stored locally	Letter recipient
		If significant, print to a Registered File and retain for 20 years	**Legal requirements:** Public Records Act	Registered File	
Policy–related correspondence	Emails discussing team or non-significant DWP business	5 years		Shared Drive	Sender or recipient as applicable
	Emails reflecting decisions on DWP policy - including attachment	20 years	**Legal requirements:** Public Records Act	Registered File	Sender or recipient as applicable
Submissions	Submissions (external)	20 years		Registered File	Policy team
	Submissions (internal)	20 years			

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time

only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix D: Retention of datasets

A data set is a collection of similar data which can be manipulated or analysed as a whole by a computer.

Retention periods start from the date when the dataset is created.

Retention of…	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Datasets	20 years after completion of the research project – unless the organisation funding the research has a different retention period.	**Legal requirements:** Public Records Act	Shared Drive or Data Warehouse	Data owner
Note: Some anonymised data sets are already archived as public records, e.g. datasets published on the DWP or gov.uk Internet sites. DWP datasets that are uploaded and accessed via the UK Data Archive. Note: all personal details must be anonymised prior to transfer to The National Archives.				

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix E: Retention of external publications (including promotional material & Legislation)

The final copy of the publication does not need to be added to the Registered File; however, you must retain in your Registered File the research and background to the publication.

Please see the publishing guidance which outlines the actions required for final published documents. Some of the items held below are held in the DWP Corporate Archive.

Retention periods start from the date when the document is created.

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Annual report	Departmental Report and Accounts	20 years	**Legal requirements:** Public Records Act	Registered File	Policy team
Consultation papers	Consultations				Policy team
Datasets - background information					Analyst team
Form (external)	Benefit forms (blank)				Forms team
Guidance (external)	Leaflets (external)				Forms team
Parliamentary documents	Command paper	20 years	**The National Archives (TNA) & legal requirements:** TNA Operational Selection Policy Osp42 - Records Of Departmental Legal Branches TNA records management retention scheduling – 12: parliamentary papers in departments and agencies Public Records	Registered File	Policy team
	Committee report				
	Directive				
	Green paper				
	House of Commons paper				
	White paper				
	Parliamentary Questions (PQs)	5 years		Shared Drive	PQ Responder
Legislation	Act of Parliament	20 years		Registered File	Policy team. **Note:**
	Statutory instrument				

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
	(SI)		Act		original signed SIs are kept by legislation team.
Press release		20 years	**TNA requirements:** TNA Retention Scheduling 8. Press and public relations records	Registered File	Press Office
Promotion materials (external)					Document creator
Public notice					
Report	Departmental reports	20 years	**TNA & legal requirements:** TNA Records and Retention Scheduling 10. Central Expenditure Records Section 386-389 of the Companies Acts 2006 Public Records Act	Registered File	Publication team
	Research - including reports, research, findings and statistics		**Legal requirements:** Public Records Act		

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix F: Retention of financial documents and data

Retention periods start from the end of the financial year to which the records relate, unless otherwise stated.

Retention of…	Specific documents	Retention period from Financial Year End	Business or legal requirements for retention	Where stored?	Who retains?
Accounts	Asset Register Including IT and non-IT.	6 years after asset disposed of	**DWP guidance:** Finance documents - retention of documents deskaid Special Payments Guide Government Procurement Card (GPC) guidance **TNA & legal requirements:** TNA Records and Retention Scheduling 10. Central Expenditure Records TNA Records Management Retentions Scheduling	RM	RM
	Finance Reports	18 months after completion of annual financial report			RM and Central Payment System (CPS)
	Financial Audits	6 years after completed			Internal audit
	Accounts - Governance Statement	6 years			Governance team
	PAYE	3 years		Stored locally	SSCL
	Payment documents & controls (as listed in the Finance Managers Guide)	6 years		Corporate Record box	Finance team
	Tax documents				Accounting

Retention of…	Specific documents	Retention period from Financial Year End	Business or legal requirements for retention	Where stored?	Who retains?
	(VAT)		3: Accounting records HMRC record keeping guidance Limitation Act 1980 Income Tax (PAYE) Regulation 2003 Section 386-389 of the Companies Acts 2006		services at SSCL
Bank account records / statements		6 years		RM & CPS	RM & CPS
Budgets (Team / Divisional and Departmental)					
Expenditure records					
Invoices	Invoices (received)			Scanned by SSCL into RM	SSCL
	Invoices (sent)	3 years		Corporate Record box	Finance team
Ledger records		6 years		Shared Drive	Finance team
Purchases	Purchase order & requisition records	6 years		RM	Procurement team / GPC card holder
	GPC receipt records	all paper documents for 18 months and all electronic documents for 7 years		Stored locally / Shared drives	
Receipts & revenue records				Corporate Record Box	

Retention of…	Specific documents	Retention period from Financial Year End	Business or legal requirements for retention	Where stored?	Who retains?
Salary records		3 years			Payroll

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix G: Retention of Human Resources (HR) documents and data

Please note: there are different retention periods for *specific* HR documents – the maximum retention period is given for the *group* of documents. See DWP HR Document Retention Schedule and DWP Health and Safety Document Retention Schedule for further details.

Retention periods start from the date when the document is created, unless otherwise stated.

Retention of document grouping… (Note: check hyperlinks for specific documents)	Maximum Retention period (for the group of documents)	Business or legal requirements for retention	Where stored?	Who retains?
Adoption leave & pay	Until age 100	**DWP guidance:** DWP HR Document Retention Schedule DWP Health and Safety Document Retention	Personal Storage Corporate record box	Line manager or recorded on RM or Employee Service Centre
Annual leave	3 years			
Attendance management	3 years			
Change of Circumstances – Individual	Until age 100			
Discipline	Until age			

Retention of document grouping… (Note: check hyperlinks for specific documents)	Maximum Retention period (for the group of documents)	Business or legal requirements for retention	Where stored?	Who retains?
	100	Schedule **The National Archives (TNA) requirements:** TNA Records Management Retentions Scheduling 2: Employee personnel records		
Employee Services forms	Until age 100			
Employment contracts	Until age 100			
Expenses	3 years			
FAMIS forms	6 years			
Flexible working hours scheme	18 months			
Grievances and Appeals	3 years			
Harassment, discrimination and bullying	3 years			
HR Mediation and Investigation Service Harassment, Discrimination & Bullying Investigation Records	3 years			
Injury leave	Until age 100			
Internal Audit and Investigations and HR Mediation and Investigation Service disciplinary investigation records	3 years			
Leaving DWP	Until age 100			
Loyalty and Recognition Awards	18 months			
Managing Poor Performance	6 years			
Maternity Leave	Until age			

Retention of document grouping… (Note: check hyperlinks for specific documents)	Maximum Retention period (for the group of documents)	Business or legal requirements for retention	Where stored?	Who retains?
	100			
Occupational Health Service Paperwork	6 years after jobholder's employment ends			
Other Documents	Until age 100			
Parental Leave	Until age 100			
Paternity Leave	12 months after Financial Year End			
People Performance	12 months (until the next appraisal year has commenced)			
Probation	6 years			
Public and Privilege Leave	12 months			
Pension (PCSPS and Superannuation)	Until age 100			
Recruitment & retention additions	Until age 100			
Sick Leave and Pay	Until age 100			
Special Leave	Until age 100			
Standards of behaviour	5 years			
Stress at Work	6 years			
Workforce Management	Until age 100			

Retention of document grouping… (Note: check hyperlinks for specific documents)	Maximum Retention period (for the group of documents)	Business or legal requirements for retention	Where stored?	Who retains?
Working Patterns and Working Time Regulations	Until age 100			

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records, DWP HR Document Retention Schedule and DWP Health and Safety Document Retention Schedule or contact the KI&RM Team.

Appendix H: Retention of legal documents

Note: See also sections on legislation-related correspondence and publications.

Note: Civil litigation is now handled by litigators at the Treasury Solicitor's Department and prosecutions by the CPS.

Retention periods start from the date when the document is created.

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Litigation	Appeals	10 years	**The National Archives (TNA) & legal requirements:** Limitation Act 1980 TNA Operational Selection Policy Osp42 - Records Of Departmental Legal Branches	Corporate Record box	DWP policy and operational leads are responsible for retaining legal advice. DWP lawyers do not keep separate registered files
	Civil litigation				
	Costs				
	Counsel				
	Employment litigation				
	Judicial Reviews				
Prosecutions		6 years			

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix I: Retention of meeting and conference documents

Retention periods start from the date when the document is created, unless an alternative retention start date is given.

Retention of…	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Agenda	1 year after meeting		Shared Drive	Document creator
Minutes	5 years		Shared Drive	
	If Registered File required – retention period is 20 years. Note: Not for publication, unsanitised or draft minutes should also be kept.	**Legal requirements:** Public Records Act	Registered File (if required)	Document creator
Meeting correspondence	4 weeks (save in inbox/sent items)		Outlook	Email creator
Presentations **Proceedings (conferences)** **Programmes (conferences)** **Speeches**	Up to 5 years If Registered File required – retention period is 20 years		Shared Drive or Registered File	Document creator

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix J: Retention of organisational & planning documents

Retention periods start from the date when the document is created, unless otherwise stated.

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Business planning	Asset Register Including IT and non-IT.	6 years after asset disposed of		Stored locally	Asset owner
	Business Continuity/ Disaster Recovery	3 years or until superseded or after 5 years print to Registered File	**DWP guidance:** Data Handling Protocol (DHP) Data Migration Plan **The National Archives (TNA) & legal requirements:** TNA Retention Scheduling 11: Internal Audit Records Public Records Act	Shared Drive	Business continuity officer
	Business Plans (department)	20 years		Registered file	Document creator
	Business Plans (team and divisional)	3 years or until superseded or after 5 years print to Registered File		Shared Drive	Document creator
	Data Protection	5 years		Shared Drive or	FoI, DPA, H&S team

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
	Act compliance (including Privacy Impact Assessments (PIA), Data Handling Protocol self service frameworks (DHP) and Data Migration Templates (DMT) – if the PIA/DHP/DMT is part of a project, project retention periods apply)			Corporate Record Box	or Document creator as appropriate
	Environmental Impact Regulations compliance				
	Freedom of Information compliance				
	Health and Safety at Work Act compliance				
	Estate management documentation	3 years or until superseded or after 5 years print to Registered File		Shared Drive	Document creator
	Governance/ Letters of Assurance		**Legal requirements:** Public Records Act		
	Risk Profiles				Risk owner

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
	Risk Register				
	Security documents				Document creator
Research documentation – including Consent forms and SARA framework		As per funding body requirements or, if significant, print to Registered File and retain for 20 years	**DWP guidance:** SARA guidance **Legal requirements:** Public Records Act	Registered File	Document creator
Diaries or calendar (Ministerial)		20 years	**TNA & legal requirements:** TNA Guidance on the Management of Private Office Papers Public Records Act	Corporate Record Boxes	Private Office
Diaries or calendar (Non-Ministerial)		1 year		Outlook or stored locally (paper diaries)	Document creator
Internal forms (templates)		3 years or until superseded or after 5 years print to Registered File		Shared drive	Document creator
IT Forms		18 months after access withdrawn	**DWP guidance:** Secure print operators	Shared drive	Document creator

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
			guide		
Mission statement		3 years or until superseded or after 5 years print to Registered File		Shared drive	Document creator
Organisation chart					
Service level agreement (SLA)		5 years after SLA ends.			
Terms of reference		5 years			
DWP Corporate Archive of historical DWP publications		Archive holdings date from 1911	**DWP guidance:** Archive collection and acquisition policy	DWP Archive & electronic copies via the Library Catalogue	DWP Archivist

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix K: Retention of policy & procedure documents

Retention periods start from the date when the document is created.

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Corporate Policy	This includes departmental policies, finance & HR policies etc.	20 years	**Legal requirements:** Public Records Act	Registered File	Policy team or guidance owners
Guidance or instructions	Finance procedures				
	HR procedures				
	Notices / Alerts				
	Operational procedures				
	Other procedures				
	Procurement procedures				

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix L: Retention of procurement documents

Note: The procurement documents are classified as per the contract value which determines the contract length.

Retention periods start when the contract ends or the last payment is made.

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Procurement - short term retention	Tender documentation	1 year	**DWP guidance:** Procurement guidance **The National Archives (TNA) & legal requirements:** TNA retention scheduling 5. Contractual records	Shared Drive	Procurement team
	Expressions of Interest and/or Pre-Qualification Questionnaires	1 year			
Procurement - involving Deeds		12 years		Corporate record box	
Procurement - over £5000	Including RTPI Catalogue forms - Ad-Hoc Request Form & POA Request Forms & Variance Request Form	6 years			
Procurement - under £5000	Including RTPI Catalogue forms - One Detail Request Form	2 years			

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.

Appendix M: Retention of programme and project documents

Retention periods start when the project/programme is completed.

Retention of…	Specific documents	Retention period	Business or legal requirements for retention	Where stored?	Who retains?
Project document - major project		20 years	**DWP guidance:** Configuration Management Plan **The National Archives (TNA) & legal requirements:** TNA Records management retention scheduling 6: project records Public Records Act	Registered File	Project manager
Project document - minor project (including LEAN projects)		10 years. If it is significant – the project documentation should be printed to paper and added to a registered file.		Corporate record box or Registered File	
Note: The Configuration Management Plan lists all the documents that should be kept in your Registered File or Corporate Record Box. **Note:** Privacy Impact Assessments (PIA), Data Handling Protocol self service frameworks (DHP) and Data Migration Templates (DMT) must be saved with the project documents if applicable.					

Note: The fact that a document doesn't **need** to be placed on a Registered File does not mean that it is not important. There may be a business need to keep the information for a particular period of time only and as such the information should be retained for example, to satisfy any management or audit checks. You may still place documents in a Registered File or a Corporate Record Box, if you decide it is significant. See Registered File Guidance for details. Registered Files are reviewed at 15 years to decide whether files should be destroyed or transferred to The National Archives.

See also section on: Retention principles of corporate records (documents and data)

For further information: see the desk aids on corporate records or contact the KI&RM Team.