Department for Digital, Culture, Media & Sport

RECORDS MANAGEMENT GUIDE -

Record retention, destruction and archiving

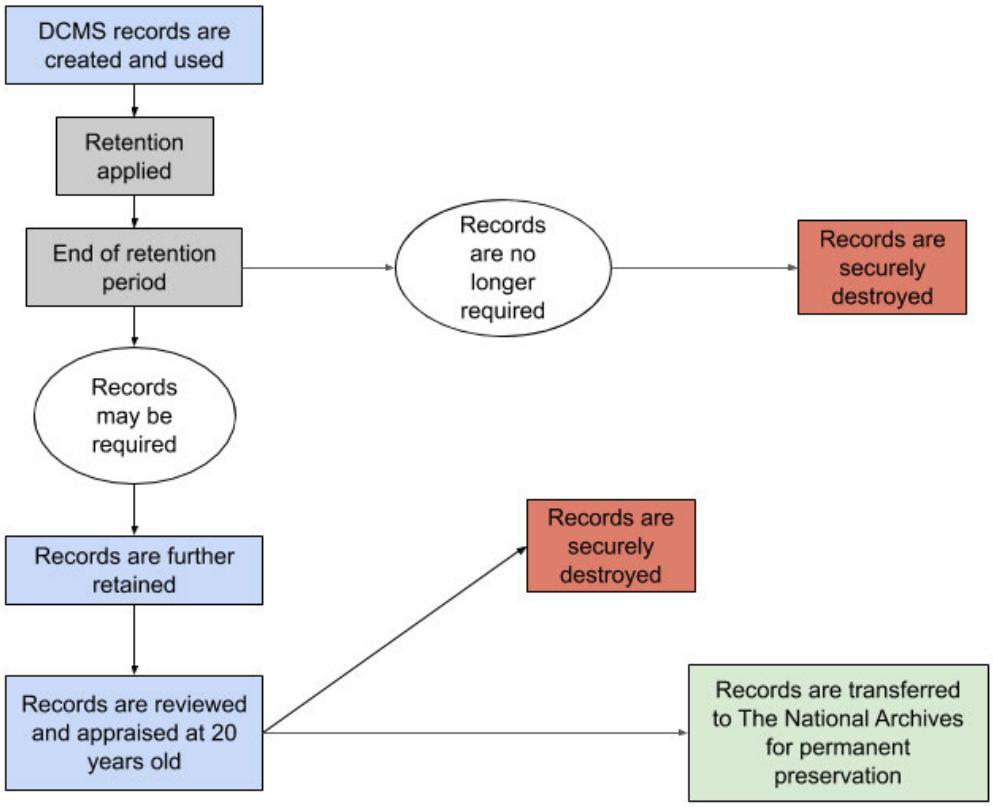
Document owner	[redacted] & [redacted]
Directorate	Digital, Data and Technology (DDaT)
Document version	2.5
Document last updated	February 2022
Document next update	March 2022
Document aim	This document will help you understand how long records should be kept for, securely destroyed and archived, as well on how to access paper files in 100PS and at the Manchester hub.

INDEX

If you are searching for something that is not covered here but think it should be, please contact the Records Team (email).

1. How long to keep records

All DCMS records have a lifespan; from creation, maintenance and use, to permanent preservation or disposal, as shown in the diagram below.



Records created within DCMS must only be retained long-term if their retention can be justified for statutory, regulatory, legal or security reasons or for their historical value. Records are not retained indefinitely for the following reasons;

- **Legal obligations under the Public Records Act 1958 and 20 year rule**
    - Public bodies must transfer records to a place of legal deposit once they are 20 years old.
- **Legal obligations under the Data Protection Act 2018 and the General Data Protection Regulation**

    - Any personal data processed must not be retained for longer than is required for its lawful purpose.
- **To support more efficient working across the department**
    - Reduction in administrative burden, ease of access to current records, freeing up of storage space.

In order to determine how long records should be kept for, DCMS has an official Record Retention Schedule (RRS) (opens in a new tab).

The RRS clarifies what information should be kept for business, legislative and historical reasons as well as helping you decide what to dispose of.

It is a legal requirement under the Freedom of Information Act 2000 for the department to have and comply with a RRS.

If you discover gaps or any incorrect information in the RRS, please contact the Records Team (email).

Please note that G-Chat messages are retained for a 90 day period, after which they are deleted.

Record moratoriums

Sometimes government departments issue moratoriums on records which prevent their destruction and may counter the RRS. When this happens, DCMS staff will be instructed appropriately:

- In 2015 a moratorium was placed (opens in a new tab) on records which may be relevant to the Independent Inquiry into Child Sex Abuse. Government departments, agencies, and public sector bodies were instructed to retain any records which contain information pertaining directly or indirectly to the sexual abuse of children or to child protection and care. This moratorium is still in place across DCMS. Please contact the Records Team (email) if you have any queries or concerns.
- DCMS is still evolving its approach to records retention and the COVID-19 inquiry, which is due to commence in Spring 2022.
    - Further information will be communicated in due course, however, it is important to be aware of the potential impact of the inquiry on records retention (opens in a new tab) and to continue to safeguard and not destroy any material that may be of potential relevance, broadly defined.

Please note that institutions have an obligation to preserve records for the Inquiry for as long as necessary to assist the Inquiry, even if they are beyond their retention period as stated on the RRS.

Prolonged retention of personal data by an organisation at the request of the Inquiry does not contravene data protection legislation, provided such information is restricted to that necessary to fulfil any potential legal duties that organisation may have in relation to the Inquiry. An institution may have to account for its previous activities to the Inquiry so retention of the data will be regarded as necessary for this purpose.

How to use the Record Retention Schedule

Staff should consult the RRS when completing the tasks below:

- Completing of the Record of Processing Activity (*annual - mandatory for IAOs [SCS1]*)
- Revising the Record of Processing Activity (*quarterly - mandatory for IAOs [SCS1]*)
- Reviewing information - see Section 2, How to review information (*annual - mandatory for teams*)
- General checking of retention periods (*as and when required - all staff*)

Records in the RRS have been arranged by the business function: Corporate Governance, Manage Estates, Manage Finance, etc.

To find a record type, either head to the relevant section or use ‘CTRL+F’ to search. For each record type listed, the retention event and period is stated. If you wish to find out the legal basis for retaining records for the period stated, please contact the Records team (email).

For example, you have found some grant funding records from eight years ago stored on your team's Shared drive and you aren’t sure what to do with them.

1. Access the Record Retention Schedule (RRS) (opens in a new tab).
2. Use ‘CTRL+F’ to search for ‘grant funding’ and find the matching entry.
3. Read the description of the section the record is listed in to make sure it is the correct record for you.
4. Use the RRS to find out the retention event and period (*six years after action completed*).
5. Confirm with your team and Line Manager whether anyone requires further access to these files.
6. If they do not require access, see Section 3, How to securely destroy records. If they do still require access, see Section 4, What to do with records you need to keep.

Broadly, records must be destroyed as soon as possible following the retention period. Failure to do so may bring DCMS into conflict with legislative and regulatory requirements.

2. How to review information

All teams should routinely review the paper and digital records they hold as a mark of good record-keeping. It is recommended that this is done on an annual basis at a time that suits the team.

It is advised that teams set up a core review group, who can liaise with the Records team should there be any queries.

How to review digital information

1. Remind your team to move any official work related content stored on their My Drives to the correct Shared drive.
2. Remind your team to save any important emails and G-chat messages to the correct Shared drive.
3. Review your team's folder structure - does it still work for the team? Could it be improved or tidied?
4. Delete any personal information that is no longer required, i.e. stakeholder contact details.
5. Ensure all files are named correctly in line with DCMS naming conventions.
6. Review files that are now closed, i.e. completed projects / events / policy work, in line with the RRS retention dates.
7. Check content within any archive folders / Shared drive(s) against the RRS for a retention date.
8. Delete files beyond the retention date, see Section 3, How to securely destroy records.
9. For files that you need to retain, see Section 4, What to do with records you need to keep

How to review paper files

If your team still routinely creates paper files, please follow the steps below;

1. Identify the location of all paper files currently stored by the team (i.e. cupboards, lockers, etc)
2. Find out what the papers are - you should keep a list with locations so that you know for next time.
3. Check the papers against the RRS for a retention date.
4. Destroy any papers beyond their retention date. See Section 3, How to securely destroy records.
5. Retain any papers which are still required / within the retention date / marked for permanent preservation or second review. See Section 4, What to do with records you need to keep.

3. How to securely destroy records

As a public body, DCMS must keep accurate and auditable records of its work and activities in order to comply with the Public Records as well as disclosure requests, such as a Freedom of Information Act request of submitting evidence to a Public Inquiry.

You should not delete any information which is of use to your team or information which may be important to DCMS now or in the future, including information which may be of historical interest to The National Archives or supports a legal requirement.

Please note it is a criminal offence to delete information that is subject to an ongoing Freedom of Information Act request.

Files should only be disposed of if they meet one or more of the following criteria:

- The retention period has expired according to the RRS
- They are draft copies
- There are duplicate copies
- They are ephemeral; there is no ongoing administrative, fiscal, legal, evidential or historical value
- There is no suspension on their destruction, i.e. a moratorium or retention order

If you are uncertain whether a file can be disposed of please contact the Records Team (email) prior to taking any action.

Deletions will be periodically monitored by the Records team to ensure DCMS is not destroying information which it is required to retain under its legal obligations.

Paper files

Official / Official-Sensitive

Paper files should be disposed of using the red confidential waste bins available on each floor at 100PS, or within the Manchester hub. If you are unclear where the red confidential waste bins are, or there is an issue with the shredder, please contact Estates (email) who will be able to assist.

Please do not destroy paper files outside of the office environment.

Secret

If you are destroying documents marked Secret, this must be done using a cross-cutting shredder and witnessed by someone from the Security team (email).

Again, please do not destroy paper files outside of the office environment.

Digital files

The Google Drive system is authorised to handle information up to Official-Sensitive. There is no distinction between how Official / Official-Sensitive information should be deleted.

1. **My Drive**

   All staff are able to delete files from their personal My Drives, although files will remain in the bin unless purposefully emptied via the ‘empty bin’ option. Once officially deleted, files are retained in Google Vault for a period of six months.

   Note: staff should not retain corporate information within their My Drives.

2. **Shared drives**

   If you are a Manager or a Content Manager of a Shared drive, you will be able to delete files. Note that files / folders will be available to restore for a period of 30 days.

   To restore a file or folder (you need at least Contributor access):

   - On the left, click a shared drive.
   - At top, next to the shared drive name, click the 'Down' arrow, and navigate to 'View trash.'
   - Select the relevant file, and navigate to 'Restore'.

3. **AODocs**

   The majority of staff across DCMS are still creating, storing and sharing information within AODocs, the third-party add-on to the Google Drive system. However, by the end of 2022, DCMS will have moved to using Shared drives as the central corporate repository.

   Please note that DCMS staff are unable to delete information from AODocs. If you have files which require deletion, please move these to a 'For deletion' folder within the AODocs library and these files will be audited and deleted by the Records team as part of the wider departmental move to Shared drives. If you do not have this folder already, you will need to create one.

4. What to do with records you need to keep

Not all files are routinely destroyed, and may need to be retained for the reasons below;

The information is beyond the retention date but staff have a legitimate business reason to hold on to it

Where a file is further required by the team beyond its retention period, the Records team (email) should be contacted in the first instance and will be able to advise whether it can be

further retained. Where the file contains personal data, the Data Protection Officer (email) should also be consulted.

All extra retention periods will be granted on a limited time basis only and are at the discretion of the Departmental Records Officer.

Examples of reasons where it may be acceptable to further retain files beyond their destruction date are listed below:

- They are required for audit purposes
- They are required for business / reference purposes for a legitimate reason
- They are required for evidence in legal proceedings
- They are required for evidence in an official inquiry

The information is marked for retention for 20 years on the RRS

This is information that has been identified as having an active long term administrative or business need, or is likely to warrant transfer to TNA, and must be retained. Please see Section 5, How to archive paper files if you have a relevant paper file and Section 6, How to archive digital files if you have a relevant digital file.

In 2012, TNA recommended that government departments create appraisal policies to identify records which should be transferred to them under the Public Records Act 1958. DCMS's Operational Selection Policy (PDF) (opens in a new tab) is available via TNA's website, although it only covers activities up until the beginning of 2017. For further information regarding appraisal at DCMS, please contact the Records team (email).

The information has not yet passed its retention date on the RRS

This information is legally required to be retained and may have ongoing administrative, fiscal, legal, evidential or historical value. If this information is no longer actively used by your team, you may wish to consider archiving options, as set out in Section 5, How to archive paper files and Section 6, How to archive digital files.

5. How to archive paper files (100 PS only)

Note: whilst colleagues largely work away from 100PS, please contact the Records team in the first instance to confirm requirements.

Paper files can be transferred to our external archive storage provider, Iron Mountain, from 100PS only. If you need to transfer paper files from another location, you will need to courier them to the Records team at 100PS - please reach out to discuss this in the first instance.

This process is closely managed by the Records team, and in order to be transferred, files must meet one or more of the following criteria:

- The file is a unique paper file, with no digital equivalent OR the file is not unique but has unique value, i.e. ministerial annotations or wet signatures.
- The file will not be required by DCMS staff on a regular / semi-regular basis.

- The file is within it's retention date and does not yet qualify for destruction.
- The file is marked for 20 year retention on the RRS.

Should you have any paper files which you think might be eligible for off-site storage, please follow the steps below:

1. Contact the Records Team (email) to confirm you meet the relevant criteria.
2. Arrange collection of boxes and labels from Room 1.74 with the Records team.
3. Pack files into the boxes.
4. Stick labels on the boxes.
5. Complete the Paper File Transfer Spreadsheet (opens in a new tab), describing the box and files. Note that the files in the box must correspond with the right SKP number on the label you applied. This is to be entered in column B.
    a. Please list each file individually.
    b. All fields are mandatory.
    c. Be descriptive.
    d. Store your spreadsheet in the appropriate team Shared drive for your area.
    e. Send your spreadsheet to the Records team.
6. Liaise with the Records team to ensure your boxes are collected and transferred to Iron Mountain.

6. How to access paper files

Note: the Records team is able to facilitate access to paper files at both 100PS and at the Manchester hub. Paper files cannot be accessed at other hub locations: if this impacts you, please contact us.

a. Requesting paper files from storage (100PS)

1. Contact the Records team (email) with either the SKP number of the box you wish to request (if known) or a series of search terms Records can use to search across the DCMS Iron Mountain catalogue to identify your files.
2. Liaise with the Records team to ensure the requested file(s) are delivered to your team's area. Delivery normally takes 48 hours from the date the request is put to Iron Mountain. Given this, we would recommend providing as much advance notice as possible.
3. Files should be accessed in a secure area, and you should not eat or drink in the vicinity of the records, in order to avoid any damage.
4. Return files to Records within one week unless otherwise agreed. Records can arrange a porter for you.

b. Requesting paper files from storage (Manchester hub)

1. Contact the Records team (email) with either the SKP number of the box you wish to request (if known) or a series of search terms Records can use to search across the DCMS Iron Mountain catalogue to identify your files.
2. Liaise with the Records team to ensure the requested file(s) are delivered. You will need to provide at least 72 hours advance notice for the files to be delivered, and liaise with the front desk at the Manchester hub to take custody of the delivery. Once you have received the delivery, you will need to confirm this with the Records team.
3. Files should be accessed in a secure area, and you should not eat or drink in the vicinity of the records, in order to avoid any damage. Within the Manchester hub, you will be permitted to access files within the [redacted] (if it is not in use) or within the printing zones. Both of these areas have secure storage space that you can use to secure files once you have finished consulting them.
4. Once you have finished with the files, you will need to contact the Records team to arrange a collection. As there will be no dedicated Records resource within Manchester, you will need to ensure that you or a trusted colleague is on site to facilitate the collection of the files. Once the files have been collected, you should confirm this with the Records team.

7. How to archive digital files

There are several options available to staff in relation to digital archive information. Please note that archive information should meet one or more of the following criteria:

- It is considered closed, and is no longer actively updated or used by the team, but legally required to be retained according to the RRS.
- It is considered closed, and is no longer actively updated or used by the team, but is marked for permanent preservation on the RRS.

If your team requires regular access to this information for reference purposes, it should not be considered archive information and should remain in the relevant Shared drive.

Teams will be responsible for regularly reviewing their archive information. It is recommended that this is done on an annual basis in line with your team's records review as set out in Section 2, How to review information.

Once information is 20 years old, it will be reviewed and potentially transferred to TNA in line with the 20 year rule and Public Records Act. This process is managed by the Records team. DCMS will begin to review its digital files in 2021, congruent to the date of the first digital record created (2000/2001).

Option 1: Files are moved to an archive Shared drive

Teams can request a new Shared drive to store archive files that meet the criteria above. Please check whether your team already has one before placing a request.

1. Raise a request for a new Shared drive via the Records team (email), providing as many details as possible.
2. Decide who needs access to the Shared drive. As this is archive information you may wish to limit this to specific team members only. Please also confirm what level of access team members require, as outlined in our sharing digital information guide (opens in a new tab).
3. Once you have access to your new Shared drive find the archive file(s) you want to move.
4. Right click on the file or select all files if you are moving multiple.
5. Select 'move to'.
6. Select Shared drives.
7. Choose the new archive Shared drive and move the file to the appropriate folder.
8. If the file has a specific destruction date on the RRS, add this to the file name or folder.

Option 2: Files are stored within an archive folder in your existing Shared drives

Teams can choose to store archive files within their existing Shared drive, however teams should store these in a separate folder to ensure ease of access and understanding of what is current across the team.

1. Create a new folder titled 'Archive' at Level 1 of your Shared drive.
2. Create any subfolders you require, for example by policy / project / event.
3. Find the file(s) you want to move.
4. Right click on the file or select all files if you are moving multiple.
5. Select 'move to'.
6. Select the folder titled 'Archive' or the relevant sub-folder to move the file.

7. If the file has a specific destruction date on the RRS, add this to the file name or folder.

.

Department for Digital, Culture, Media & Sport

RECORDS MANAGEMENT GUIDE - How to store digital information

Document owner	[redacted] & [redacted]
Directorate	Digital, Data and Technology (DDaT)
Document version	3.5
Document last updated	February 2022
Document next update	March 2022
Document aim	This document will help you understand archiving digital files and folders, deleting information, saving emails and G-Chat messages to Drive, storing personal information and version control of documents.

INDEX

If you are searching for something that is not covered here but think it should be, please contact the Records Team (email).

1. Archiving digital files and folders

You should ‘archive’ any files which your team does not require frequent access to, but needs to keep. Reasons for archiving may include:

- They may be required for reference purposes in the future, i.e. event planning;
- They are of historical importance and may be of interest to The National Archives, i.e. policy papers;
- You are legally required to retain them for a period of time according to the department’s Records Retention Schedule (opens in a new tab).

Please see our Records Management Guide for Retention, Destruction and Archiving (opens in a new tab) for detailed information on how to archive digital files. You may wish to nominate someone in your team to manage this process.

The Public Records Act 1958 requires central government departments to identify records of historical value and transfer them for permanent preservation to The National Archives by the time they are 20 years old.

DCMS continues to develop its approach to how we will review and transfer our digital information to The National Archives. Any relevant updates will be relayed to staff as and when required.

2. Deleting information

As a public body, DCMS must keep accurate and auditable records of its work and activities in order to comply with the Public Records as well as disclosure requests, such as a Freedom of Information Act request of submitting evidence to a Public Inquiry.

You will not routinely need to delete information from AODocs libraries or Shared drives, unless the file or folder contains personal information, duplicate or draft documents or ephemeral information.

You will need at least 'Content Manager' permissions to delete information from a Shared Drive and deletions can be audited.

To delete anything from AODocs, please email the Records team (email).

You should not delete any information which is of use to your team or information which may be important to DCMS now or in the future, including information which may be of historical interest to The National Archives or supports a legal requirement.

Please note it is a criminal offence to delete information that is subject to an ongoing Freedom of Information Act request.

Personal information may need to be deleted more often, in line with agreed retention schedules.

Please see our Records Management Guide for Retention, Destruction and Archiving (opens in a new tab) for further information on how to delete files.

If you are uncertain if information should be deleted or have a query regarding the deletion of personal data, please email the Records team (email).

4. Saving Chat messages to Google Drive

It is your responsibility to decide what Chat messages are important and should be saved into your team's Shared drive to form part of the record.

DCMS' retention policy states that Chat messages are retained for 90 days, after which they are deleted. You should therefore review your Chat messages regularly to ensure that any important information is captured within this period.

You should save Chat messages to the appropriate AODocs library or Shared drive if:

- It provides evidence of an important decision
- It will be useful for your team/future team members
- It supports DCMS in meeting an operational or legal obligation
- You think it might be of historical interest to The National Archives

Please follow the instructions below to save Chat messages:

1. Login to your email account
2. In the textbox, type "in:chats" and press enter. This will retrieve all messages present within Chat.
3. Select the chat logs you would like to save and open them. They will then open in as a threaded email conversation.
4. Select 'Print.'
5. In the destination field, choose 'Save as PDF' and click 'Save.'
6. Name your email using the DCMS Naming Conventions (opens in a new tab) and save it to your desktop or downloads folder.
7. Find the folder you want to save the email to in your AODocs library, Shared drive or My Drive.
8. Select 'New' and choose 'File upload' and find the email you saved.
9. After uploading, you should make sure to delete the pdf. from your harddrive.

5. Storing information in Google Drive

Government information must be appropriately protected at all times. Read the Government

Security Classifications (opens in a new tab) policy to find out how you should safely keep and share information.

You should also complete the Security and Data Protection course on Civil Service Learning every year.

Google Drive is authorised to store information up to the OFFICIAL level of security classification, including any OFFICIAL information that is also marked as OFFICIAL-SENSITIVE.

Nearly all DCMS work has the OFFICIAL security classification. You do not need to mark information you keep in Google Drive as OFFICIAL.

A small amount of OFFICIAL information is of a particularly sensitive nature, this is information where loss or disclosure would have damaging consequences to an individual, an organisation or a government department.

Examples of information that should be marked OFFICIAL-SENSITIVE include:

- the most sensitive corporate or operational information, for example relating to organisational change planning, contentious negotiations, or major security or business continuity issues
- commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to DCMS or to a commercial partner if improperly accessed
- sensitive information about operations or equipment that could damage capabilities or effectiveness
- policy development and advice to ministers on contentious and very sensitive issues
- information about investigations and civil or criminal proceedings that could disrupt law enforcement or prejudice court cases
- sensitive diplomatic business or international negotiations

Access to sensitive information must be no wider than necessary, limited to those with a business need-to-know. This ‘need to know’ principle applies wherever sensitive information is collected, stored, processed or shared.

You should clearly mark any files or folders that contain sensitive information in Google Drive as ‘OFFICIAL-SENSITIVE’.

Sometimes the file title can be just as sensitive as the information contained within the file. For example a file called ‘John Smith Disciplinary’ offers sensitive information about John Smith. Make sure you only send and share sensitive information with the right people, even if they cannot access it.

[redacted]

Department for Digital, Culture, Media & Sport

RECORDS MANAGEMENT GUIDE

Use of Collaboration Tools

Document owner	[redacted] and [redacted]
Directorate	Digital, Data and Technology (DDaT)
Document version	1.3
Document last updated	February 2022
Document next update	March 2022
Document aim	This document outlines DCMS' approach for managing data held in collaboration tools and SaaS products. DCMS users should use this guide to help them use collaboration tools securely and better manage information.

Index

If you are searching for something that is not covered here but think it should be, please contact the Records Team (email).

Introduction

Collaboration tools including those provisioned on DCMS devices or cloud-based (SaaS) tools can enable collaborative working across a range of disciplines. However, unless explicitly stated in policy, these collaboration tools are not considered to be official DCMS corporate repositories and therefore staff must adhere to the below guidance when using these tools to support their work.

Principles

- Use the tool securely and protect the data held within it;
- Use collaboration tools inline with other departmental policies, including the DCMS IT Acceptable Use Policy (opens in a new tab) and the Security Handbook (opens in a new tab);
- Exhibit behaviours that adhere to the Civil Service Code (opens in new tab); do not use defamatory or abusive language or act in any way that may cause distress to an individual or reputational damage to the department;
- Support the department to continue to meet its obligations under the Data Protection Act 2018, Public Records Act 1958 and Freedom of Information Act 2000;
- Do not use collaboration tools for the purposes of processing personal data without approval from the Operational Data Protection Team (email);
- Some tools will not be suitable for use and may be prohibited. If you are unsure if you can use a tool, contact the IT team (email);
- Follow the guidance for Civil Servants on “Using cloud tools securely”, https://www.gov.uk/guidance/using-cloud-tools-securely (opens in new tab).

Guidance

This guidance should be used to support staff manage DCMS information held in collaboration tools, either provisioned on DCMS devices or cloud-based (SaaS) tools.

Controlling access to information

- You should continually review who has access to tools and revoke access where its no longer required;
- You could implement a joiners, movers, leavers process to ensure that access is always up to date;
- If you move role or leave DCMS and no longer require access, you should remove your access and close your account;

Finding information

- You must ensure that information is accessible to those who need access to it;
- You should regularly review the content of tools and move any relevant information into a formal corporate repository. For DCMS, this is Google Drive;
- If you are answering a disclosure request, you will need to consider whether there is any relevant information held in a tool and export that data to Google Drive.

Information ownership

- If you are collaborating with another department, ALB or external organisation you should decide who is responsible for managing the data;
- In some cases, a formal data sharing agreement or Memorandum of Understanding (MOU) will be required. For more information, contact the Operational Data Protection Team (email).

Retention of data

- Most of these tools are not official corporate repositories, so data is not subject to a specific data retention policy unless specifically set out in DCMS retention schedule (opens in a new tab);
- You should regularly review information in tools and move important information to Google Drive;
- You could set up a process to regularly capture important information e.g. weekly, monthly or yearly depending on your use of the tool.

Public Records Act 1958

- As a civil servant, you must keep accurate records of your work;
- In order to do this, records must be captured in official corporate repositories. For DCMS this is Google Drive.

Digital continuity

- Many tools - particularly cloud-based - will not be supported by DCMS IT team so you should ensure that information in a tool does not become lost or inaccessible over time;
- The best way to prevent loss or damage to information is to move it as soon as possible to Google Drive so it can be properly managed.

Manage Relationships > Internal

Code	Name / Description / Record Examples	Jurisdiction	Retention Event	Official Retention Period
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
PR-INT-040	**Google Chat Instant Messages**	GB	The date that the message is sent.	90 Days