

# Data Retention and Erasure Policy

Version 1: 26<sup>th</sup> April 2018



# INTRODUCTION

The Council accumulates vast amounts of data, of numerous types, including but not limited to, planning applications, claims, assets, correspondence, statements, legal documents, contracts, and financial records.

The data is held in a range of forms such as letters, emails, contracts, deeds, plans and can be physical ie hard copy or electronic.

Certain information may need to be retained for one or more of the following reasons:

- To meet operational needs,
- to fulfil statutory or other regulatory requirements,
- is evidence of agreements or events in the case of a dispute, or
- to preserve documents of historic or other value

Some of this information is personal data about living individuals.

The introduction of the General Data Protection Regulation (GDPR) now brings new requirements to consider relating to the retention of personal data, with the emphasis being around minimization of data (in terms of the volume of data held about individuals and the length of time that the data is held for). Data breaches carry considerable risk of reputational damage and financial penalties of up to €20 million.

Article 5(e) of the GDPR states that:

*'personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historic research purposes or statistical purposes in accordance with Article 89(1) subject to implication of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*

In addition to this, Recital 39 of the GDPR also states:

- *'In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review'*

Therefore, in order to meet our GDPR data retention obligations we need to ensure that:

- we are retaining information appropriately in order to fulfil our requirements, but
- we DO NOT retain personal data for longer than we are permitted to,

By having concise retention guidelines in place and ensuring that they are followed, will also remove the risk of personal data being processed after its permitted period (therefore removing a further risk), and ensures Chorley Council is meeting legal requirements (reducing the risk of financial fines being imposed as a result of breaches and the associated risks of reputational damage).

At the end of the retention period it is important to ensure that the information is disposed of in the most appropriate manner

Article 6(1) of the GDPR details lawfulness of processing and states that processing is lawful if at least one of the following applies:

- a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

- b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The lawfulness of processing being relied upon is an important factor when considering the retention period and must be taken into account.

## **DATA RETENTION APPROACH**

The Council understands the importance of data being stored safely and for the correct period of time.

The creation of clear, concise guidelines will ensure that staff acting as Data Controllers understand the data retention requirements applicable to the data they decide the purpose and means of processing for and an appropriate data retention period can be determined and justified.

The Council will ensure personal data is securely disposed of when no longer needed.

The purpose of this policy is to ensure the Council is compliant with GDPR data retention obligations and will remain compliant in the future.

This policy will ensure that necessary data, records and documents the Council collate and hold are adequately protected and maintained and to ensure that records that are no longer needed or are of no value are discarded at the proper time. This policy is also for the purpose of aiding employees of the Council in understanding their obligations in retaining data or electronic documents including email, web files, text files, sound and movie files, PDF documents and all Microsoft Office or other formatted files.

In summary, personal data will be retained for no longer than is necessary. A Corporate Data Retention Schedule will be produced by the Council as well as individual teams within each Directorate to demonstrate a generic retention period based on the purpose of the data and data retention guidelines. Each Service within the Council will have its own Retention Schedule (as set out at Appendix 1) based on the data each team holds.

In the event that the retention of personal data is no longer necessary for the operation of the Council, the data shall be deleted and all copies shall be destroyed as per the defined schedule

## **POLICY OBJECTIVES**

The objective of this policy is to assist officers of Chorley Council with the management, retention and disposal / destruction of records and information (particularly where personal information is included), held as either hard copy or held electronically:

- To ensure the Council operates in an appropriate manner that results in the Council meeting its legal obligations and thus remaining GDPR compliant
- To prevent premature destruction of information that needs to be retained for a specific period in order to satisfy a financial, legal or other requirement of public administration.

- To assist in identification of information that may have future value and is worth preserving for archival purposes.
- To promote an improved and consistent approach to data retention and destruction.

## **SCOPE**

This policy applies to all personal information held by the Council and to all Council staff who handle documentation and process information.

## **POLICY STATEMENT**

The Council will ensure that:

- it does not keep information for longer than is necessary
- it will retain the minimum amount of information required in order to carry out its statutory duties
- personal data is securely disposed of when no longer needed
- data will be disposed of in the most appropriate and agreed manner.

This will be achieved by Council staff adhering to the following:

- The retention of paper documents / hard copies will be kept to an absolute minimum.
- General files will no longer be allowed to be kept by staff. This is because they are impossible to interrogate once they have attained a certain size and is inefficient. GDPR asks Data Controllers to identify personal data and by keeping general files this will make it harder to be GDPR compliant. There is a risk that the Council will not be GDPR compliant.
- Wherever possible, paper documents (hard copies) will be scanned in and stored as a digital / electronic version and the paper (hard copy) will be disposed of in an appropriate manner (see below for further information). This will be carried out as quickly as possible after receipt of documents.
- Wherever possible, paper documents (hard copies) should not be kept on desks, lockers, drawers or trays.
- Unless specified otherwise in the Corporate Retention Policy, or any Service Retention Policies or documented Retention Schedules, paper documents / hard copies of documentation will be disposed of as follows:-
  - Contains confidential and commercially sensitive information - shredded onsite
  - Contains personal data – shredded onsite
  - Contains no confidential or personal data – disposed of in recycle (where possible) waste containers
  - Public documents, not containing confidential and / or personal information – disposed of in (recycle, where possible) waste containers
  - When documents are being disposed of on someone else's behalf, clear guidance should be provided as to how the documents should be disposed of, and in the absence of such guidance, documents should be shredded onsite.
- A register of destruction of records should be kept. Enough detail should be recorded to identify which records have been destroyed, it is not sufficient to record that a certain quantity of records was been destroyed on a particular date.

- If documents are to be shredded off-site by a 3rd party organisation, appropriate checks must have taken place to ensure their suitability to handle the data and arrangements documented. At the end of the data destruction process, the 3<sup>rd</sup> party organisation will supply on request, a Certificate of Destruction.
- Certain types of documents do not need to be, and indeed should not be retained at all wherever possible; this can include, unnecessary duplicated copies, trivial (normal course of business' type) emails, documents of no importance such as compliment slips, flyers, advertisements, compliment slips. It should be considered normal practice to dispose of these types of documents as soon as possible.
- Duplicated and superseded materials for instance, draft documents and minutes of meetings that have now been finalised can be destroyed without a retention period (and is deleted as 'normal course of business').
- The period for which personal data is stored should be limited to a strict minimum and time limits should be established by the data controller for deletion of the records (referred to as erasure in the GDPR) or for a periodic review. For further information regarding these time limits, please refer to Service specific Data Retention guidelines and Data Retention Schedule.

## ADMINISTRATION

The following Record Retention Schedule is the initial maintenance, retention and disposal schedule for records held by the Council. This schedule should be reviewed regularly (every 6 months) to ensure the data retention policy approach is adhered to. The same applies to Service specific retention schedules.

There are certain occasions when information needs to be preserved beyond any limits set out in the policy. The policy must be SUSPENDED relating to a specific customer or document and the information retained beyond the period specified in this Data Retention Schedule in the following circumstances:

- Legal proceedings or a regulatory or similar investigation or obligation to produce information are known to be likely, threatened or actual
- A crime is suspected or detected
- Information is relevant to a company in liquidation, receivership or where a debt is due to the Council
- Information is considered by the owning unit to be of potential historical importance

In the case of possible or actual legal proceedings, investigations or crimes occurring, the type of information that needs to be retained relates to any that will help or harm the Council or the other side's case, liability or amount involved.

If there is any doubt over whether legal proceedings, an investigation or a crime could occur or what information material is relevant in these circumstances, the Council shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.

## RESPONSIBILITIES

The responsibilities of our people are detailed below:

Roles	Responsibility	Frequency
All officers	Ensure that any correspondence received via post, or delivered in person to the Council offices, is actioned. If the documentation needs to be retained, ensure that it is scanned	Ongoing

(All Directorates)	in and stored electronically on any appropriate CRM system and the paper copy of the document, is securely disposed of.	
	To action emails received from members of the public, or that contain personal information as soon as possible and to then delete the email once fully actioned (and no longer required).  If the email needs to be retained, ensure that it is stored electronically on any appropriate CRM system and the original email deleted from officers mailbox.	Ongoing
	Ensure paper records are kept to an absolute minimum and to avoid storing in personal drawers, lockers, desk and trays wherever possible.	Ongoing
Line Managers / Team Leaders	Ensure staff are routinely reminded of the responsibilities covered above.	On-going
(All Directorates)	Ensure staff receive training and support where appropriate	
Data Controllers / Information Asset Owners	To be aware of regulatory requirements relating to the retention of data they collect and store	On-going
(All Directorates)	To notify the GDPR Compliance Officer of statutory / regulatory changes that occur relating to the retention of the data held by their Directorate	On-going
	Ensure that all personal data is retained and disposed of, is done so in line with GDPR and statutory requirements.	On-going
HR Manager	To ensure HR / staff records are retained and disposed of, in line with GDPR and statutory requirements.	On-going
Health and Safety Officer	Ensuring that all Health and Safety records are retained and, when appropriate, disposed of in line with GDPR and statutory requirements.	On-going
Directors/Heads of Service	Ensuring that all teams are complying with GDPR; ensuring that Data Retention Schedules are completed; ensuring that the Council's suppliers and contractors demonstrate GDPR compliance and that they check their credentials and guarantees. As a controller the Council need to have a written contract that explicitly defines each parties responsibilities and liabilities. Importantly, data controllers are always liable for the compliance with GDPR.  In addition, if the Council operate outside the EU the Council need to document the location of the controlling authority within the EU. Contracts with suppliers, verification and ongoing management are key to long term GDPR compliance.	On-going
Chief Executive	Overall Officer level responsibility for data retention	On-going
Audit	Work with ICT to review batch deletion to ensure it is functioning appropriately and that a suitable audit trail is	Annually

	recorded.	
	To carry out internal audits to ensure Services are adhering to policy, to report findings, and make recommendations for improvements that can be made	On-going
	Undertake spot checks as identified in the risk assessment	Ongoing
Policy & Communications	Ensuring that Marketing Strategies and Events are compliant with GDPR and keeping Staff updated.	On-going
ICT Manager	The Information Manager will have overall responsibility for maintaining systems capable of batch deletion of information that has reached its retention limit.	As required
	Work with Audit to review batch deletion to ensure it is functioning appropriately and that a suitable audit trail is recorded.	Annually

## MONITORING AND REVIEW ARRANGEMENTS

This policy will be reviewed annually (or as required following legislative changes).

## RECORD RETENTION SCHEDULE

The data retention policy is based on the following schedule.

### DEPARTMENT / FUNCTION

- A. Accounting and finance
- B. Contracts
- C. Corporate records
- D. Correspondence and internal memoranda
- E. Personal information
- F. Electronic records
- G. Insurance records
- H. Legal
- I. Miscellaneous
- J. Personnel records
- K. Tax records

### A. Accounting and Finance

Record Type	Retention Period
-------------	------------------

Annual audit reports and financial statements	permanent
Annual audit records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual plans and budgets	2 years
Bank statements and cancelled cheques	7 years
Employee expense reports	7 years
Interim financial statements	7 years
Credit card records (documents showing customer credit card number)	2 years

All records showing customer bank details must be locked in a desk drawer or a filing cabinet when not in immediate use by staff. If it is determined that information on a document, which contains credit card information, is necessary for retention beyond 2 years, then the identifying details will be cut out of the document.

#### **B. Contracts**

<b>Record type</b>	<b>Retention Period</b>
Contracts and related correspondence (including any proposal that resulted in the contract and all other supportive documentation)	7 years after expiration or termination

#### **C. Corporate Records**

<b>Record type</b>	<b>Retention Period</b>
Corporate records (minutes, signed minutes of the board and all committees, record of incorporation, articles of incorporation,	permanent



annual corporate reports)	
Licenses and permits	permanent

#### **D. Correspondence And Internal Memoranda**

General principle: most correspondence and internal memoranda should be retained for the same period as the document to which they relate. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded within two years. Some examples include:
  - Routine letters and notes that require no acknowledgment or follow up, such as notes of appreciation, congratulations, letters of transmittal and plans for meetings
  - Form letters that require no follow up
  - Letters of general inquiry and replies that complete a cycle of correspondence
  - Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change)
  - Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary
  - Chronological correspondence files

Copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed; unless that information provides reference to, or direction to other documents and must be kept for project traceability.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be permanently retained.

#### **E. Retaining Personal Information**

This section sets out the data retention policies and procedure that are designed to help ensure compliance with legal obligations in relation to the retention and deletion of personal information

Personal information that is processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The Council will usually delete personal data falling within the categories set out below at the date/time set out below:

<b>Record type</b>	<b>Retention period</b>
Information about a computer and about visits to and use of this website (including an IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths)	2 years following account closure
Information provided when registering with our website (including email address)	2 years following account closure
Information provided when completing a profile on our website (including a name, gender, date of birth, interests and hobbies, educational details)	2 years following account closure
Information provided for the purpose of subscribing to email notifications and/or newsletters (including a name and email address)	Indefinitely or until the client chooses to 'unsubscribe'
Information provided when using the services on the website or that is generated in the course of the use of those services (including the timing, frequency and pattern of service use)	Indefinitely
Information relating to any subscriptions made (including name, address, telephone number, email address and card details)	2 years following account closure
Information posted to our website for publication on the internet	2 years after post
Information contained in or relating to any communications sent through the website (including the communication content and metadata associated with the communication)	2 years following contact
Any other personal information chosen to be sent	2 years following contact

Notwithstanding the other provisions of this section, the Council will retain documents (including electronic documents) containing personal data:

- to the extent that we are required to do so by law;
- if we believe that the documents may be relevant to any ongoing or prospective legal proceedings;
- and in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk).

The Council will run database backups of all electronic data contained on our servers. This backup will include all information relating to all current users, as well as any information that remains on the server due to any reason contained in this policy. This database backup is a safeguard to retrieve lost information within a one year retrieval period should system users experience any problems.

## **F. Electronic Documents**

Electronic mail: not all email needs to be retained and, it depends on the subject matter.

- All emails from internal or external sources are to be deleted after 12 months
- Staff will strive to keep all but an insignificant minority of their emails related to business issues
- We will archive emails for six months after the staff have deleted it, after which time the email will be permanently deleted
- Staff will take care not to send confidential/proprietary information to outside sources

Electronic Documents: including Microsoft Office Suite and PDF files. Retention also depends on the subject matter.

- PDF documents - The length of time that a PDF file should be retained should be based upon the content of the file and the category under the various sections of this policy. The maximum period that a PDF file should be retained is 6 years. PDF files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace
- Text/formatted files - Staff will conduct annual reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those they consider unnecessary or outdated. After five years, all text files will be deleted from the network and the staff's desktop/laptop. Text/formatted files the staff deems vital to the performance of their job should be printed and stored in the staff's workspace

We do not automatically delete electronic files beyond the dates specified in this policy. It is the responsibility of all staff to adhere to the guidelines specified in this policy. In certain cases a document will be maintained in both paper and electronic form. In such cases the official document will be the electronic document.

## **G. Insurance Records**

<b>Record Type</b>	<b>Retention Period</b>
--------------------	-------------------------

Certificates	permanent
Claims files (including correspondence, medical records, injury documentation, etc.)	permanent
Insurance policies (including expired policies)	permanent

## H. Legal Files and Papers

Record Type	Retention Period
Legal memoranda and opinions (including all subject matter files)	7 years after close of matter
Litigation files	1 year after expiration of appeals or time for filing appeals
Court orders	permanent
Contracts	10 years
Requests for departure from records retention plan	10 years
Register of Members	permanent
Minutes of Director's meetings	10 years

## I. Miscellaneous

Record Type	Retention Period
-------------	------------------

Consultant's reports	2 years
Material of historical value (including pictures, publications)	permanent
Policy and procedures manuals – original	Current version with revision history
Policy and procedures manuals copies	Retain current version only
Annual reports	permanent
Record of persons I.D. for money laundering purposes	5 years
Any work related reportable accident, injury or death	3 years from report
Immigration checks	2 years from termination of job

#### **J. Personnel Records**

<b>Record Type</b>	<b>Retention Period</b>
<p>Job applications/interviews of unsuccessful candidates</p> <p>Note: Application forms should give the opportunity for subjects to object to their details being retained/processed.</p>	6 months or less (longer with explicit consent).

Employee personnel records (including individual attendance records, annual leave, application forms, job or status change records, performance evaluations, termination papers, withholding information, garnishments, test results, training and qualification records)	6 years after separation
Employment contracts – individual	7 years after separation
Employment records correspondence with employment agencies and advertisements for job openings	3 years from date of hiring decision
Job descriptions	3 years after superseded
Working time opt-out forms	2 years
Current bank details of employees	Only as long as necessary

## K. Tax Records

General Principle: Donors forum must keep books of account or records as are sufficient to establish amount of gross income, deductions, credits or other matters required to be shown in any such return. These documents and records shall be kept for as long as the contents thereof may become material in the administration of tax laws.

Record Type	Retention
Tax-exemption documents and related correspondence	permanent
Tax bills, receipts, statements	7 years
Tax returns	permanent
Sales/use of tax records	7 years
Annual information returns	permanent
Payroll/wage records for unincorporated businesses	5 years after 31 January following the year of assessment

PAYE records	3 years (minimum) from
Maternity records	3 years after the end of the tax year in which the maternity pay period ends

The above retention periods apply in all cases. The default retention period unless otherwise specified for any data item is 7 years, after which time the data should be securely deleted.





Reason: Please detail if retention action is statutory or common practice (Standard practice followed by local authorities who are members of the Records Management Society); quote any other useful information such as relevant Acts.

Retention Period/Action: Please detail any statutory periods the data must be retained for, or quote agreed periods that data will be held for (eg, 1 yr after last administrative use). Please state “Permanently” for data that must be kept indefinitely, or for approximately 100 years, for legal and/or administrative purposes, and/or are of enduring value for historical research purposes.

Disposal / Destruction guidelines: Please detail how data is disposed once the Retention period is reached