Data Retention and Erasure Policy

Last updated May 2023

South Ribble Borough Council | Chorley Council

WORKING TOGETHER

Contents

Document Control

Version	Date	Reason for Change	Amended by
1.0	03/23	Creation of document.	Head of ICT
1.1	12/04	Reviewed by Director of Governance.	Director of Governance
1.2	01/05	Approved by SMT	Head of ICT

Next Review Date: March 2024

This policy applies equally and jointly to each authority, however the data will be processed locally.

1. Purpose and Scope

The Council has large volumes of data.

The data is held in various formats both physical and electronically.

Some information may need to be retained. Acceptable reasons for retention are:

- To meet operational needs.
- To fulfil statutory or other regulatory requirements.
- Evidence of agreements or events in the case of a dispute.
- To preserve documents of historic or other value.

Some of this information is personal data about living individuals.

The General Data Protection Regulation (GDPR) places a greater emphasis on the minimisation of data. This means the volume of data held about individuals and the length of time this data is held for.

By having data retention guidelines in place and ensuring these are followed reduces the risk of personal data being processed after its permitted period, therefore reducing the overall risk to Chorley Council and South Ribble Borough Council (Council). 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.

2. Objective

The objective of this policy is to assist officers 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.

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

3. 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 staff ensuring:

- The retention of paper documents / hard copies are kept to a minimum.
- Wherever possible, paper documents (hard copies) will be scanned electronically with the paper (hard copy) disposed of in an appropriate manner.
- Unless specified otherwise in the Corporate Retention Policy, or any Service Retention Polices paper documents / hard copies of documentation will be disposed of as follows:

Type of Data	**Disposal Method**

Contains confidential and commercially sensitive information	Shredded onsite
Contains personal data	Shredded onsite
Contains no confidential or personal data	Recycled
Public documents, not containing confidential and / or personal information	Recycled
When documents are being disposed of on someone else's behalf, clear guidance should be provided as to how the documents are being disposed of. In the absence of such guidance, documents should be shredded onsite.	Shredded onsite

A register of destruction of records should be kept. Enough detail should he recorded to identify which records have been destroyed.

If documents are to be shredded off-site by a 3rd party organisation as data processors appropriate checks (by the data controller – the Council) must have taken place to ensure their suitability to handle the data and arrangements documented. At the end of the data destruction process, the 3rd party organisation will supply on request, a Certificate of Destruction.

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').

4. Responsibilities

Roles	**Responsibility**	**Frequency**
All officers (All Directorates)	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 in and stored electronically on any appropriate CRM system and the paper copy of the document, is securely disposed of.	Ongoing
	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 (All Directorates)	Ensure staff are routinely reminded of the responsibilities covered above.	Ongoing
	Ensure staff receive training and support where appropriate.	Ongoing
Data Controllers / Information Asset Owners (All Directorates)	To be aware of regulatory requirements relating to the retention of data they collect and store.	Ongoing
	To notify the GDPR Compliance Officer of statutory / regulatory changes that occur relating to the retention of the data held by their Directorate.	Ongoing
	Ensure that all personal data is retained and disposed of, is done so in line with GDPR and statutory requirements.	Ongoing
HR Manager	To ensure HR / staff records are retained and disposed of, in line with GDPR and statutory requirements.	Ongoing
Health and Safety Officer	Ensuring that all Corporate Health and Safety records are retained and, when appropriate, disposed of in line with GDPR and statutory requirements.	Ongoing
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.	Ongoing
Chief Executive	Overall Officer level responsibility for data retention.	Ongoing
Audit	Work with ICT to review batch deletion to ensure it is functioning appropriately and that a suitable audit trail is recorded.	Annually
	To carry out internal audits to ensure Services are adhering to policy, to report findings, and make recommendations for improvements that can be made.	Ongoing

	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.	Ongoing
Head of ICT	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

5. Data Retention Schedule

The Councils data retention schedule can be viewed on the Councils website.