Data Usage 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	14/04	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 recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The Data Protection Act 2018 and UK GDPR has introduced changed to the rights of individuals who we hold data about.

We need to ensure we communicate with both internal and external customers about how we will use their data. This includes how it will be used, how it will be stored, how long it will be retained and the rights they have relating to that data.

Article 13 of the GDPR sets out what information we must provide when we are collecting personal data from a data subject; it specifies we must provide the following information at the point when the data subject provides their personal information:

- Who we are (when acting as Data Controller) and our contact details.
- Contact details of our Data Protection Officer.
- The purposes of the processing for which personal data are intended, as well as the legal basis for the processing.
- If applicable, the legitimate interests.
- The recipients or categories of recipients of the personal data, if any.
- If we intend to transfer personal data to third countries or international organisations.
- For what period the personal data will be stored; or if that's not possible, the criteria used to determine that period.
- Of their right to request access to held information.
- Of their right to rectification.
- Of their right to erasure of personal data (where applicable).
- Of their right to restriction of processing (where applicable).
- Of their right to data portability.
- Of their right to withdraw consent (where applicable).
- Of their right to lodge a complaint with the supervisory authority (ICO).

- Whether the provision of personal data is a statutory or contractual requirement, whether the Data Subject is obliged to provide the personal data and of possible consequences of failure to provide data.
- The existence of any automated decision making. If automated decision making is used, we must provide meaningful information about the logic involved, the significance and envisaged consequences of such processing for the Data Subject.

Article 13 also explains that we must notify the data subject if we intend to further process the personal data for a purpose or purposes other than that for which the personal data were originally collected.

Article 14 also sets out requirements when personal data is obtained but is not directly obtained from the data subject. The same information must be provided as detailed above, however, rather than being provided at the point when the data subject provides the information, instead it must be provided:

- Within a reasonable period after obtaining the information, at least within one month, having regard to the specific circumstances in which the personal data are processed.

- If disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed.

- If personal data are to be used for communication with the data subject, at the latest at the time of the first communication with the data subject

For information, Article 4(1) of the GDPR defines personal data as:

'personal data means any information relating to an identified or identifiable nature person ('data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'

Essentially this is information from which an individual person can be identified.

The purpose of this policy is to identify appropriate and inappropriate use of data and to ensure Chorley Council and South Ribble Borough Council (Council) meets its requirements of advising data subjects of the rights available to them.

We must inform individuals:

- How we will process their data.

- If their data will be shared.

- Of the rights they are entitled to.

- The required contact details.
- How long data will be stored for.
- Whether submission of personal data is a statutory or contractual requirement.
- Of any automated decision making which takes place.

2. Principles

The principles of this policy are to create a set of guidelines that will detail:

- The information we need to provide to individuals when they provide personal information to us.
- The information we will communicate to individuals when we receive their data via another channel.
- When and how the information will be communicated.

This policy applies to all personal information held by the Council.

3. Roles and Responsibilities

The table below details the roles and responsibilities:

Role	Responsibility	Frequency
All officers (All Directorates)	Ensure they are aware of and understand the wording of the Privacy Notice and digital opt-in arrangements	Ongoing
	Will make their line manager aware, if they become aware of any problems with the Privacy Notice webpage / opt-in function	Ongoing
Line Managers / Team Leaders (All Directorates	Ensure their staff are aware of and understand the Privacy Notice	On-going
	Ensure any problems reported or identified with the Privacy Notice webpage / function are reported to ICT as soon as possible	On-going
Data Controllers (All Directorates)		On-going
		On-going
Data Protection Officer	Is aware of any changes to the GDPR, particularly those which may result in the amendments to the Privacy Notice	On-going
Directors/Heads of Service		

Chief Executive	Overall Officer level responsibility	
Internal Audit	Produce reports following internal audits, with recommendations for improvements in procedures	On-going
	Undertake spot checks as identified	On-going
Policy & Communications		Bi-annually
	Undertake spot checks as required and identified in the risk assessment	On-going
ICT Team	The Head of ICT will have overall responsibility for ensuring online notifications such as Privacy Notices displayed as webpages and digital opt-in arrangements are operational	As required
	To carry out necessary work to ensure webpage-based Privacy Notice and digital opt-in arrangements are functioning correctly and remain operational	As required