Data Protection Policy

Document Control

Document Title	Data Protection Policy
Document Owner	Information Assurance
Author	Stephen Weaver / Alexandra West
Created	June 2023
Approved by	*Information Governance Board*
Review Cycle of Document	Bi-annually
Document Classification	Official
Document Distribution	All staff
Next Document Review Date	June 2025

Version Control

Revision History			
Version	**Date**	**Reason for issue**	**Issued By**
0.9	July 2021	Initial release	
1.0	June 2023	2 Yearly Review	Alexandra West/Stephen Weaver

About this policy

The Data Protection Policy lays out the principles for ensuring that the Council meets its obligations under the General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA 2018), as well as other related data protection laws.

Contents

About this policy 1
Purpose 1
Definitions 1
Scope 2
Policy Statements 2
Individual's Responsibility 3
Policy Compliance 3
Exceptions 3

Purpose

The purpose of this policy is to ensure that the council is committed to compliance with all relevant data protection laws in respect of personal data and to protecting the rights and freedoms of individuals whose information the Council handles. The Council's compliance with this legislation is underpinned by the six data protection principles.

In summary, the principles require that personal data is:

1. processed fairly, lawfully and in a transparent manner
2. used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes
3. adequate, relevant, and limited to what is necessary
4. accurate and, where necessary, up to date
5. not kept for longer than necessary
6. kept safe and secure

In addition, the accountability principle requires the Council to be able to evidence its compliance with the above six principles and make sure that individuals are not put at risk because of the way the Council handles their personal data.

There are a number of policies, operational procedures and guidance documents provided to staff to give them appropriate direction on the application of the data protection legislation - these are listed in the Information Governance Framework.

Non-compliance with this Policy could expose the Council and/or its customers to unacceptable risk.

The potential impact of damage or loss of information includes disruption to services, risk to citizens (including risk to life), damage to reputation, legal action, personal distress, financial penalties, loss of confidence, and/or media coverage and may take considerable time and cost to recover.

Definitions

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Pseudonymised personal data is covered by the legislation; anonymised data, provided that and meaning the anonymisation is irreversible, is not classed as personal data and therefore does not fall under the UK GDPR.

Some personal data (called special category data) is more sensitive and is afforded more protection; this is information relating to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;

- Health data;
- Sexual life and/or sexual orientation;
- Criminal offence data (convictions and offences).

Scope

The policy applies to all users of the Council's information. Non-compliance with the policy and other relevant policies in the IG Framework could expose the Council and/or its customers to risk.

Policy Statements

The Council is committed to transparent, lawful, fair and proportionate processing of all personal data it handles.

The following list covers key areas of data protection and how the Council deals with them.

Privacy Notices
The Council will publish privacy notices on its website and provide timely notices where this is required. We track and make available any changes in our privacy notices. Staff privacy notices are also published and kept up to date.

Training
All staff are required to attend data protection and security training as part of their induction, as well as annual refresher training. Additionally, staff are required to undertake specialised information governance and security training relevant to their job role.

Breaches
The Council takes the management of personal data breach incidents very seriously and has a reporting mechanism that is communicated to all staff. The Council has a process which determines whether a data breach needs to be reported to the ICO as the Regulator. We take appropriate action to make data subjects aware where necessary.

Information Rights
The Council has clear processes to handle information rights requests, including subject access requests. There is a dedicated team who have enhanced training in this area.

Data Protection by Design and Default
There are documented processes to assist staff in ensuring compliance with all privacy by design principles. This includes procedures to assess the risks when processing personal data (Data Protection Impact Assessment –DPIA). The Council has mandated the use of DPIAs for the following:

- Planning to adopt new technologies that process personal data
- Carrying out systematic and extensive profiling or automated decision-making to make significant decisions about people;
- Processing special-category data;

- Systematic monitoring of publicly accessible place, e.g. CCTV

Records of Processing Activities (ROPAs)
The Council will have a comprehensive register of all its records of processing activities (RoPA) to ensure information risks and relevant technical and organisational controls are captured. This will be maintained by Information Asset Owners (those responsible for Information Asset and Risk Management).

IG Framework – Policies and Procedures
There is a suite of policies, procedures and guidance that underpin the data protection policy within the Council. These are communicated to all staff at induction and stored on the organisation's intranet. The Information Governance Framework policy lists the documents that form the IG Framework, defines the intended audience and whether or not the documents are mandatory.

Communications
The Council has a clear communication plan which seeks to embed a culture of privacy, data protection and information risk awareness.

Contracts
The Council's legal department oversee that contracts are compliant with the UK GDPR where relevant. This includes data processing agreements with suppliers who provide services to the Council.

Individuals' Responsibility

It is the responsibility of individuals to ensure that they understand privacy issues and data protection issues, as well as the sensitivity of the data being handled. Users will gain a better understanding of this by attending the new starter induction, as well as annual refresher training for IG, and are alert to messaging from the Information Assurance team.

There are a number key groups and roles that underpin the Council's approach to protecting personal data. These are set out in the Information Governance Framework.

Policy Compliance

The Council requires that all employees comply with the directives presented within this policy. This policy will be included in the GDPR/Data Protection and Information Security Internal Audit Programme and compliance checks will take place to review the effectiveness of its implementation.

Exceptions

SIRO exceptions may be granted to parts of this policy where emergencies arise.

In such circumstances, individuals must contact their line managers and ensure that the actions taken are recorded and reported to the IG Team as soon as possible.