Data Protection Policy

Author: Valerie Smith
Version: 13
Review/Revision date: May 2025

1. Introduction

Almost everything we do in a data-driven world involves the sharing of personal data, from a name, address or birth date to sensitive information such as sexuality, health and biometrics. Data may be shared in an increasing number of ways, including verbally, electronically, when visiting a website, using social media or sending an email.

While using and sharing personal data helps make life easier, more convenient and connected, personal data belongs to the person whose information it is. The Data Protection Act (DPA) 2018 and UK General Data Protection Regulation (UK GDPR) give legal rights to people about how their personal data is used.

The personal data we handle may relate to individual people, a group of people, past and present employees, contractors and other organisations. In whatever role we use personal data; it must only be used in ways that comply with the law and which the person concerned would reasonably expect. It must also be kept safe.

This applies to all types of collection of personal data, both physical and virtual; whether held on paper, electronically or recorded in some other way. Data Protection legislation prescribes how the Council must look after that information.

This Policy sets put how the Southend-on-Sea City Council (the Council) will fulfil its duties regarding the protection of personal data.

2. Contribution to Southend 2050 Ambition and the Council's Values and Behaviours

Through the data protection process we help the Council to display the behaviours of being innovative while taking a sensible approach to risk, using good judgement and behaving responsibly with personal data. This allows citizens, employees, businesses and partners to have trust when engaging with the Council.

While underpinning all Southend 2050 outcomes which involve the use of personal data, our work in particular relates to:

Safe and Well – enabling people in all parts of the City to feel **that we will keep their personal data safe**

Opportunity and Prosperity – Ensuring our **workforce is skilled at handling personal data properly**

Connected and Smart – Southend is a **leading digital city** where personal data is used to provide digital age services innovatively but ethically

3. Policy Statement

The proper processing of personal information by the Council is very important to successful operations and to maintaining confidence in the Council and the services it provides.

The Council fully endorses and adheres to the key principles set out in the UK GDPR and will meet them by taking the following approach:

Lawfulness, fairness and transparency

We will identify valid grounds under data protection legislation for collecting and using personal data and record these in our Record of Processing Activities (RoPA).

We will ensure we do not do anything with the data that breaches other laws.

We will use personal data in a way that is fair (not processing data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned).

We will be clear, open and honest with people from the start about how we will use their data and will explain our intentions in a Privacy Notice.

Purpose Limitation

We will be clear from the start about our purposes for processing data and explain these in a Privacy Notice.

We will record our purposes in our Record of Processing Activity (RoPA).

We will only use personal data we have gathered for a new purpose if either it is compatible with our original purpose, if we get consent or if we have a clear obligation or function laid out in law.

Data Limitation

We will ensure that the personal data we process is:

- Adequate (sufficient to properly fulfil our stated purpose)
- Relevant (has a rational link to that purpose)
- Is limited to what is necessary (we do not hold more information than we need for that purpose)

Accuracy

We will take all reasonable steps to ensure the personal data we hold is correct and is not misleading as to any matter of fact.

We will keep personal data updated where there is a need to do so.

We will take reasonable steps to correct or erase incorrect or misleading personal data.

We will carefully consider any challenges to the accuracy of personal data.

Storage Limitation

We will not keep personal data for longer than we need it.

We will consider how long the personal data we hold needs to be held and why.

We will periodically review the data we hold and erase or anonymise it when it is no longer needed.

We will carefully consider any challenges to our retention of data.

Integrity and confidentiality (security)

We will ensure that we have appropriate technical and organisational security measures in place to protect the personal data we hold.

Where appropriate we will use measures such as pseudonymisation and encryption.

The measures we take will be appropriate to the analysed risk, our polices and will include both physical and technical measures.

We will ensure the confidentiality, integrity and availability of our systems and services and the personal data we process within them.

We will ensure we can restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

We will test the effectiveness of our measures and undertake any required improvements.

We will not transfer personal data outside the UK or European Economic Area without suitable and adequate protection being in place.

Accountability

We will take responsibility for what we do with people's personal data.

We will adopt a 'data protection by design and default' approach to our business.

We will put written contracts in place with organisations that process personal data on our behalf.

We will maintain documentation of our processing activities.

We will record and, where necessary, report personal data breaches.

We will carry out data protection risk assessments for uses of personal data that are likely to result in high risk to individual's interests.

We will appoint a Data Protection Officer.

We will adhere to relevant codes of conduct.

We will ensure appropriate records are in place to demonstrate our compliance to the Information Commissioner, if required.

We will review and, if necessary, update the measures we have in place.

4. Special Category and Criminal Convictions Data

Special category and criminal convictions personal data is given additional protection under the legislation. Special category data is defined as personal data about an individual's:

- Race
- Ethnic origin

- Political opinions
- Religious of philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Health data
- Sex life
- Sexual orientation

Criminal convictions data is defined as personal data relating to an individual's criminal convictions and offences or related security measures and includes personal data relating to:

- The alleged commission of offences by the data subject
- Proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

We will ensure we comply with data protection legislation when processing such data.

5. Sensitive Processing for Law Enforcement Purposes

When processing sensitive data for law enforcement purpose we are required to take extra steps to ensure we comply with the law enforcement data protection principles contained in the DPA 2018.

'Law enforcement purposes' means processing for the purpose of the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public safety.

For law enforcement purposes, 'sensitive processing' means:

- The processing of personal data revealing:
    - Racial or ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade union membership
- The processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual
- The processing of data concerning health
- The processing of data concerning an individual's sex life or sexual orientation

We will ensure we comply with data protection legislation when processing such data for law enforcement purposes.

6. Individual Rights of Data Subjects

We will ensure that people are able to fully exercise their rights as a data subject under the Act. These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making including profiling

7. The Council's roles when using personal data

The Council is a **Data Controller** because, in carrying out many of our functions, we decide for ourselves how and why we use people's personal data.

For some purposes the Council joins together with third parties to share people's personal data in order to accomplish an outcome. In these instances, the method and purpose of sharing personal data is agreed jointly. Each party remains a Data Controller (as they independently decide how and why they use personal data in each instance). This is sometimes referred to as being a **Joint Controller**.

The Council may also ask a **third party to act as a Data Processor for us**. In this instance we must require them to follow our instructions about the way any personal data concerned may be used.

The Council sometimes **acts as a Data Processer for a third party**, carrying out tasks for them, following their instructions about the appropriate use of personal data.

8. Sharing Personal Data

There are occasions when it is beneficial to share an individual's personal data with a third party. This might, for example, be so that we can deliver a service to that person, safeguard their wellbeing or to protect public funds. Alternatively, sharing may be required for a statutory purpose such as the prevention and detection of crime.

We will comply with data protection legislation when deciding whether to share personal data, either on a one-off basis or as a regular arrangement and will record when personal data has been shared. Formal information sharing agreements will, where beneficial, be put in place to document the extent and nature of the data sharing.

9. Services provided by a third party

Where any party is to process personal data on our behalf, we will ensure there is a written agreement including, for example, the type of personal data they will be processing, the limits put on the use they may make of that data, the period during which the processing is authorised and what will happen at the end of the agreement to the personal data gathered on our behalf.

We will take steps to ensure that a third party is reputable and will take proper care of the data we are asking them to process.

This applies to any person or body acting on behalf of the Council, regardless of whether it is a charged-for service. Where there is a contract, we will ensure that the Council's standard data protection clauses and schedule are included. Where there is no contract, we will assure ourselves that the third party will meet all data protection obligations.

10. Marketing, promotion and advertising

When we use personal data to contact people to offer services and opportunities, we will ensure that we meet our obligations regarding data protection. Where there is no alternative basis for the data processing, we will ensure that we have the person's explicit consent to make contact (other legislation should also be considered when issuing marketing material).

11. Research and Analysis

When using personal data for research or analysis purposes we will be ethical in our approach and will minimise the data we use by, wherever possible, using anonymisation, pseudonymisation or statistical techniques. In this way we will preserve the privacy of the individuals whose personal data is being used while ensuring the benefits which can be realised from research and analysis are delivered.

12. Data Protection awareness and skills

Managers will ensure that all staff are aware of their responsibilities regarding the proper use and safeguarding of personal data and that this is part of their terms and conditions of employment.

A baseline of knowledge will be ensured through mandatory data protection training which will be made available to all staff. Where necessary training will be adapted in its form or delivery to allow for those staff who are unused to working on a computer or whose use of personal data in the workplace is minimal. Training should take place as part of the induction process for new staff and annually for all others.

Some people will require specialist training such as the SIRO, Caldicott Guardian, Data Protection Officer and Councillors.

As part of the analysis of data security incidents and complaints, the Information Governance, Complaints and Resolution Service will decide whether training needs have been identified. This may be on an individual, team or broader basis.

Where a matter relating to data protection is identified where disciplinary action may be appropriate, HR services will advise and support managers as necessary.

13. Complaints about Data Protection matters

Where a complaint is made regarding whether the Council has met the statutory rights of data subjects, an investigation or review will be carried out by the Information Governance, Complaints and Resolution Service, in conjunction with the service area. This will take preference over the Council's complaints procedure. The nature of the investigation or review will vary according to the subject matter of the complaint; procedures are described in the relevant supporting policy or procedure.

Should a complainant be dissatisfied with a data protection related matter which does not relate to their statutory rights, or where there is dissatisfaction with the manner in which their complaint about a statutory matter has been handled, the Council's complaint procedure may be used.

Where a complaint is made to the Information Commissioner's Office (ICO), the Information Governance, Complaints and Resolution Service will co-ordinate a response.

14. Governance of Data Protection

The Governance Board (which includes the Caldicott Guardian and SIRO) will monitor high level compliance with this policy. They or their supporting groups will receive the following reports:

Cyber Security matters (from ICT)

Subject Access Request performance (from DPO)

Data Security Incidents, themes and lessons learned (from DPO)

Emergency Planning and Business Continuity matters (from Resilience Manager)

In addition, any other matter regarding data protection may, where necessary, be considered by the Governance Board.

Reports will be made to Caldicott Board meetings as required, in particular concerning data security incidents in the field of social care.

A summary of performance in relation to data protection matters will be reported annually to Councillors in the Information Governance Update and SIRO Report made to Cabinet (and any subsequent scrutiny committee).

15. The role of the Data Protection Officer and their team (the Information Governance, Complaints and Resolution Service)

As a local government body, the Council is required by data protection legislation to appoint a Data Protection Officer (DPO). The Data Protection Officer will, supported by their team, assist Southend-on-Sea City Council by:

- Monitoring the internal compliance of the Council with its responsibilities as a Data Controller under the Data Protection Act 2018, General Data Protection Regulation (and any variation made to that legislation).
- Informing and advising on data protection obligations, in particular through policies, awareness raising, training and audits

- Providing risk management guidance, in particular advice regarding Data Protection Impact Assessments and their monitoring
- Acting as a contact point for data subjects, employees and the Information Commissioner
- Assisting in demonstrating compliance and accountability with data protection responsibilities

Under their statutory duty, the Data Protection Officer may report their concerns regarding data protection compliance to the Chief Executive or other senior manager, if matters cannot be resolved through usual channels.

16. Other Support and advice

ICT will provide specialist advice and support to the organisation concerning cyber security. They will also be responsible for and advise on ensuring the integrity of the Council's ICT systems and architecture. Where ICT systems are obtained outside of the ICT portfolio, managers are responsible for ensuring their suitability with regard to data protection.

Procurement services will provide assistance with the data protection elements of Council contracts, with specialist support from the Data Protection Risk Support Service where required.

17. Supporting Policies and Procedures

The matters in this policy are expanded upon in a series of supporting policies and procedures which can be found on the Information Governance pages of the intranet.

Key Roles and Responsibilities

Senior Information Risk Officer (SIRO)

The SIRO is the Executive Director for Strategy and Change. They take overall ownership of the Council's information management framework and have specific responsibility to:

- Ensure compliance with regulatory, statutory and organisational information security policies and standards
- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with Council's risk management framework
- Act as the champion for information risk within the Council
- Establish a reporting and learning culture to enable the Council to understand where issues exist and develop strategies, policies, procedures and awareness campaigns, to prevent problems occurring in the future

Privacy Officers

The Privacy Officer is the Director of Digital and ICT. They oversee all on-going activities related to the development, maintenance of, and adherence to data protection legislation and guidance. This includes all policies and procedures related to the processing of, and access to personal data.

Caldicott Guardian

The Executive Director for Adults & Communities acts as the Council's Caldicott Guardian. This responsibility was introduced following the 1997 Review of the Uses of Patient-Identifiable Information, chaired by Fiona Caldicott which sets out six (now eight) Caldicott Principles on information governance as well as requiring the appointment of Caldicott Guardians.

Data Protection Officer

The Customer Support Manager, Information Governance, Complaints and Resolution Hub is the Data Protection Officer for the Council and is responsible for advising the organisation about data protection legislation, providing guidance and monitoring compliance.

They are the Council's point of contact (link officer) with the Information Commissioner's Office.

Governance Board (GB)

A group with overall responsibility for ensuring the organisation has appropriate governance for its functions. All the above post holders are members of the GB.

Version Control

Date	Version	Reason	Owner	Author
August 2014	V8	Amendments after review	Lysanne Eddy	Indi Viknaraja
April 2018	V 9	Partial update to reflect GDPR/DPA 2018	Lysanne Eddy	Val Smith
January 2020	V10	Reviewed and updated to include more comprehensive content linking to supporting policies, procedures and guidance.	Val Smith	Val Smith
November 2021	V11	Reviewed and updated to include change to the Caldicott Guardian	Val Smith	Val Smith
May 2022	V12	Reviewed and updated to reflect City status and change of SIRO and PO.	Val Smith	Val Smith
May 2023	V13	Reviewed and updated to reflect rebrand, change of Caldicott Guardian and current information governance structure	Val Smith	Karen Finn

Purpose:	To specify how the Council complies with data protection legislation when processing personal data
Status:	Final
Date:	May 2023
To be reviewed by:	May 2025
Governance:	Governance Board