Data Protection Policy

Version & Policy Number	Version 3.0
Guardian	Data Protection Officer
Date Produced	April 2024
Next Review Date	June 2025

Approved by Cabinet	

SUMMARY OF DOCUMENT

Rutland County Council is committed to protecting the rights and privacy of individuals, including service users, staff, and others, in accordance with the United Kingdom General Data Protection Regulation (UK GDPR).

The UK GDPR contains provisions that we will need to be aware of as data controllers, including provisions intended to enhance the protection of service users' personal data. For example, the UK GDPR requires that the Council has privacy notices that are written in a clear, plain way that staff and service users can understand.

Rutland County Council needs to process certain information about its staff, service users and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- The recruitment and payment of staff.
- The administration of services.
- Collecting payments and fees.
- Complying with legal obligations.

To comply with various legal obligations, including the obligations imposed on it by the UK GDPR, Rutland County Council must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Contents

1.0 INTRODUCTION

Background

1.1 Rutland County Council (RCC) needs to collect person-identifiable information about individuals to carry out its functions and fulfil its objectives.

1.2 Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly.'

1.3 Personal data can include data relating to employees (present, past, and prospective), service users, contractors and third parties, private and confidential information, and sensitive information, whether in paper, electronic or other form.

1.4 Irrespective of how information is collected, recorded and/or processed person- identifiable information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulations (UK GDPR).

1.5 The DPA and the UK GDPR require RCC to comply with the key Data Protection Principles and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually.

1.6 The DPA and the UK GDPR give rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, to ask us to stop using it, in certain permitted circumstances, and to seek damages where we are using it improperly.

1.7 The lawful and correct treatment of person-identifiable information by RCC is paramount to maintaining the confidence of its service users and employees. Compliance with this Policy will enable RCC to ensure that all person- identifiable information is handled and processed lawfully and correctly.

Data Protection and the UK GDPR Principles

1.8 RCC has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The Council also has a duty to comply with guidance issued by the Information Commissioners Office.

1.9 All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to the Council. Significant financial penalties can be imposed upon the Council and/or its employees for non-compliance.

1.10 The aim of this Policy is to outline how the Council meets its legal obligations in safeguarding confidentiality and adhering to information governance requirements. The obligations in this Policy are based on the DPA and UK GDPR requirements, as the key legislative and regulatory provisions governing the security of person-identifiable information.

1.11

2.0 WHAT INFORMATION IS COVERED

2.1 Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly.' Individuals can be identified by various means including their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

3.0 POLICY STATEMENT

3.1 This Policy applies to all person-identifiable information obtained and processed by the Council, its employees, Members, and agents.

It sets out:

- The Council's policy for the protection of all person-identifiable information that is processed
- The responsibilities and best practice for data protection
- The key principles of the DPA and the UK GDPR.

4.0 PRINCIPLES

4.1 The objective of this policy is to ensure the protection of information the Council keeps in accordance with relevant legislation, namely:

- To ensure notification;

Annually notify the Information Commissioner about RCC's use of person-identifiable information.

- To ensure professionalism;

All information is obtained, held, and processed according to the DPA and the UK GDPR.

- To preserve security;

All information is obtained, held, disclosed and disposed of in a secure manner.

- To ensure awareness;

Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

- Data Subject access;

Prompt and informed responses to subject access requests

4.2 The policy will be reviewed periodically by the Council's Data Protection Officer. Where review and update are necessary due to legislative changes this will be done immediately.

5.0 SCOPE OF THIS POLICY

5.1 The Policy covers all person identifiable information, electronic or paper which may relate to employees, Members, contractors and/or third parties about whom the Council holds information.

6.0 POLICY

6.1 RCC obtains and processes person-identifiable information for a variety of different purposes., including but not limited to:

- Staff records and administrative records
- Service Users records include the administering of benefits, council tax, housing records, elections, grants, planning applications, licensing applications etc.
- Matters relating to the prevention, detection and investigation of offences, fraud, and corruption
- Matters relating to the enforcement of primary and secondary legislation
- Complaints and requests for information.

6.2 Such information may be kept in either computer or manual records. In processing such personal data, RCC will comply with the data protection principles within the DPA and UK GDPR.

7.0 DATA PROTECTION RESPONSIBILITIES

Overall Responsibilities

7.1 The Council is the 'data controller' and permits its staff to use computers and relevant filing systems (manual records) in connection with their duties. The Council has legal responsibility for the notification process and compliance with the DPA and the UK GDPR.

7.2 The Council, whilst retaining its legal responsibilities, has delegated data protection compliance to the Data Protection Officer who can address concerns about the data held by the Council and how it is processed, held, and used.

Elected Members

7.3 When members process personal data whilst acting as a representative of residents of their electoral ward and /or whilst representing a political party, they do so independently of the council's registration with the Information Commissioner. However, where an elected member has access to and processes personal information on behalf of the Council, the member does so under the Council's registration and must comply with this Policy.

Chief Executive and directors

7.4 The Chief Executive and Strategic Directors are responsible for implementing safe data protection procedures within their services and the operation of those services and ensuring the proper security of information held. Strategic Directors should have regard to The Data Protection Policy, the Information Governance Framework and the Acceptable IT Use Policy when formulating any policies or procedures which make use of personal data.

Data Protection Officer's (DPO) responsibilities

7.5 The Council appoints a Data Protection Officer (DPO), who is available to address any concerns regarding the data held by the Council and how it is processed, held, and used.

The DPO is responsible for ensuring that the Council's registration is kept accurate. Details of the Council's registrations can be found on the Office of the Information Commissioner's website. Compliance with the legislation is the personal responsibility of all staff who process personal information.

Information Governance Officer

7.6 The Information Governance Co-Ordinator has specific responsibility for data protection compliance and for advising and training on data protection matters. The Information Governance Officer shall report to the Data Protection Officer.

Senior Information Risk Owner

7.7 The Senior Information Risk Owner (SIRO) has strategic responsibility for governance in data protection risk. The SIRO:

- Acts as advocate for information risk at the Corporate Leadership Team.
- Oversees the reporting and management of information incidents.

The SIRO will assist the organisation to consider the information risks associated with its business goals and how those risks will be managed.

All Staff Responsibilities

7.8 All staff must ensure that their working practices comply with the Data Protection principles and that the information held by the council is accurate and up to date.

7.9 All new staff will receive basic training on data protection as part of their induction. Managers should ensure all staff for whom the manager is responsible receive appropriate training on Data Protection legislation, on the application of this Policy and on their individual responsibilities.

General responsibilities

7.10 All officers are subject to compliance with this Policy. Under the UK GDPR individuals can be held personally liable for data protection breaches.

7.11 All officers must inform their line manager and the Data Protection Officer of any data incident, as soon as practicable after it has been identified.

7.12 All officers will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Compliance Officer.

7.13 Officers must follow the subject access request procedure

8.0 SECURITY OF DATA

Information Access

8.1 All staff are responsible for ensuring that personal data which they use, or process is kept securely and is not disclosed inappropriately.

Access to personal data should only be given to those who have and can show a need for access to the data for the purpose of their duties.

All officers and members are responsible for ensuring that any personal data they see or hear is not disclosed to third parties unless there is clear and specific authority. This includes personal data and information extracted from such data, for example, unauthorised disclosure of data might occur by passing information over the telephone, communicating information contained on a computer print-out or by allowing it to be read on a computer screen.

Acceptable IT use

8.2 All officers and members must ensure that they have read and comply with the ICT Email and Security Policy and the ICT Security Policy, which must be signed as read by all staff before access to information containing personal data is permitted.

Hard copy data

8.3 Documents containing personal data must be stored securely.

Data destruction

8.4 Personal data which is no longer required must be destroyed confidentially. Computers must have all personal information securely deleted using the appropriate software tools. Personal data must be destroyed in accordance

with the council's retention protocol.

Remote Working

8.5 The security and proper processing of data outside offices and usual places of work, and whilst travelling, must be ensured.

Data breaches

8.6 Personal data security breaches will be detected, reported, and investigated in accordance with the Data Incident Response Policy.

9.0 CONDITIONS AND LAWFULNESS OF PROCESSING INFORMATION

Lawfulness of processing

9.1 To meet the 'lawfulness' requirement, processing personal data must satisfy at least one the following conditions:

- The data subject has given consent
- The processing is required due to a contract
- It is necessary due to a legal obligation
- It is necessary to protect someone's vital interests (that is, life or death situation)
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority
- It is necessary for the legitimate interests of the council or a third party

Processing of special categories of personal data

9.2 Special category data is personal data, which is deemed more sensitive under UK GDPR, and so needs more protection. This covers information concerning racial or ethnic origin; political opinions; religious and philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; data concerning health and sex life and sexual orientation.

For special categories of personal data, at least one of the following conditions must also be met:

- The data subject has given explicit consent
- The processing is necessary for the purposes of employment, social security, and social protection law
- The processing is necessary to protect someone's vital interests
- The processing is carried out by a not-for-profit body
- The processing is manifestly made public by the data subject
- The processing is necessary for legal claims
- The processing is necessary for reasons of substantial public interest
- The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services

- The processing is necessary for public health
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards

10.0 ACCOUNTABILTY AND GOVERNANCE

Data protection by design and default

10.1 To ensure that all data protection requirements are identified and addressed when designing new systems and processes, or when reviewing or expanding existing systems or processes, an approval process must be undertaken before continuing. This process is called a data protection impact assessment (DPIA).

The DPIA process helps to identify and minimise the data protection risks of a project. A DPIA must be undertaken where processing information is likely to result in a high risk to individuals, but it is good practice for assessments to be carried out for any other major projects which require the processing of personal data.

A DPIA must:

- Describe the nature, scope, context, and purpose(s) of the processing
- Assess necessity, proportionality, and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks

Record Management

10.2 Good record management plays a pivotal role in ensuring the Council can meet its obligations to provide information and retain it in a timely and effective manner to meet its legal requirements.

It is necessary to ensure that robust record management practices are in place which are understood and implemented by all staff.

It is the responsibility of all staff to ensure that they are familiar with the policies, procedures and schedules relating to record management within the council, including the Document Retention and Records Management Policy. All records should be retained and disposed of in accordance with the Council's Document Retention Schedules.

11.0 COMPLIANCE MONITORING

11.1 Compliance with this policy will be monitored by the Strategic Director of Law and Governance, together with reviews by Internal Audit where necessary.

11.2 To confirm that an adequate level of compliance is being achieved by services/departments in relation to this Policy, the Council will carry out regular data audits of service areas. Each audit will, as a minimum, assess compliance with this Policy in relation to the protection of personal data, including:

- The assignment of responsibilities
- Raising awareness
- Training of employees
- The effectiveness of data protection related operational practices
- Personal data transfers
- Data Breach management
- Personal data complaints handling
- The level of understanding of data protection policies and privacy notices
- The currency of data protection policies and privacy notices
- The accuracy of personal data being stored

12.0 REVIEW

12.1 The council will process personal data in accordance with all applicable laws and applicable contractual obligations. The council will only process personal data in accordance with the requirements of this Policy. The Data Protection Officer is responsible for the monitoring, revision and updating of this document every 2 years or sooner if the need arises.

Rutland County Council
Catmose, Oakham, Rutland LE15 6HP

01572 722 577
enquiries@rutland.gov.uk
www.rutland.gov.uk