Data Protection Policy

Status: OFFICIAL

Owner: Data Protection Officer (DPO)

Approver: Executive Management Team

Version: V1.0, dated 20th May 2026

Applies to: All employees, elected Members, temporary staff, contractors, agents and any other persons processing personal data on behalf of the Council.

---

1. Purpose

The Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) establish the legal framework for the lawful processing of personal data and the protection of individuals' privacy rights.

The Council is committed to ensuring that all personal data is processed lawfully, fairly and transparently and is committed to protecting the privacy of individuals. This policy sets out:

- The Council's corporate commitments and governance arrangements for data protection; and
- The expectations placed on officers and elected Members when handling personal data as part of their duties.

Compliance with this policy is mandatory. Failure to comply may result in legal or regulatory consequences for the Council and, where appropriate, disciplinary action.

---

2. Scope

This policy applies to all personal data processed by or on behalf of the Council, regardless of format, including electronic, paper and other records.

Personal data is information about a living individual who can be identified from the data.

This policy applies to all processing activities undertaken by:

- Employees;
- Elected Members;
- Temporary and agency staff;

- Contractors and agents; and
- Third parties acting on the Council's behalf.

Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

In some circumstances, the Council may operate as a joint controller with another organisation, or as a data processor acting on the instructions of another data controller. Such arrangements must be clearly documented, and roles and responsibilities agreed in writing in accordance with the UK GDPR.

---

3. Data Protection Principles

All processing of personal data **must** be carried out in accordance with the following UK GDPR principles:

1. **Lawfulness, fairness and transparency** – processing must be lawful and fair and personal data must be processed in a transparent manner.
2. **Purpose limitation** – personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data minimisation** – personal data collected must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
4. **Accuracy** – personal data must be accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
5. **Storage limitation** – personal data must not be retained for longer than necessary for the purposes for which it is processed.
6. **Integrity and confidentiality (security)** – personal data must be processed securely and protected from unauthorised or unlawful processing, and against accidental loss, destruction or damage using appropriate technical or organisational measures.
7. **Accountability** – the Council must be able to demonstrate compliance with all data protection requirements under the UK GDPR.

---

4. Lawful Basis for Processing

Before collecting or using personal data, officers must identify and record a lawful basis for processing under Article 6 of the UK GDPR, and under Article 9 of the UK GDPR for 'sensitive' personal data.

The lawful bases most commonly relied upon by the Council are:

- **Public Task** – processing necessary to perform statutory or official functions;
- **Legal Obligation** – processing required to comply with the law or other legal obligation;
- **Contract** – processing necessary to enter into or perform a contract; and
- **Consent** – used only where no other lawful basis applies.

4.1 Consent

Consent should not be relied upon where there is a power imbalance or where processing is necessary to deliver Council services. In order for consent to be valid it must be 'fully informed', which means that the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or when an individual is under duress.

Where processing is based on consent, individuals have the right to withdraw consent at any time. Withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn.

4.2 Special category data

Where special category data or criminal offence data is processed, an additional condition under Article 9 (and where applicable Article 10) of the UK GDPR must be identified, and an **Appropriate Policy Document** maintained where required.

The UK GDPR defines special as:

- personal data revealing **race or ethnic origin**
- personal data revealing **political opinions**
- personal data revealing **religious or philosophical beliefs**
- personal data revealing **trade union membership**
- **genetic data**
- **biometric data** (where used for identification purposes)
- data concerning **health**
- data concerning a person's **sex life**
- data concerning a person's **sexual orientation**

Where criminal offence data is processed, such processing must be authorised by law and meet a condition set out in Schedule 1 of the DPA.

---

5. Roles and Responsibilities

To support clarity and accountability, the table below summarises the key data protection roles within the Council and their core responsibilities.

Role	Key Responsibilities
Council (Corporate Body)	Acts as Data Controller; ensures compliance with data protection legislation; adopts and maintains appropriate policies and governance arrangements.
Data Protection Officer (DPO)	Provides advice on data protection obligations; monitors compliance; advises on DPIAs; oversees breach and complaint handling; acts as contact point with the ICO.
Executive Management Team (EMT)	Monitors compliance with data protection requirements; ensures that the Council's has appropriate technical and organisational measures in place.
Corporate Information Governance Group (CIGG)	Chaired by the Director of Finance and Corporate Services enabling information governance issues and lessons learned to be cascaded to all areas of the organisation and any significant issues reported to EMT
Assistant Directors / Lead Specialists	Ensure processing activities have a lawful basis; are covered by privacy notices; are recorded in the Record of Processing Activities and Information Asset Register; ensure staff compliance within their service areas.
Officers and Members	Process personal data only where there is a lawful basis and it is necessary; comply with all policies and training requirements; keep data secure; report breaches or concerns immediately.
Contractors / Third Parties	Process personal data only in accordance with written agreements and Council instructions; apply appropriate security measures; report incidents or breaches without delay.

5.1 The Council

The Council is the data controller and is legally responsible for ensuring that all personal data is processed in accordance with data protection legislation.

5.2 Data Protection Officer (DPO)

The Council has appointed a Data Protection Officer in accordance with Article 37 of the UK GDPR. The DPO is responsible for:

- Advising the Council, Members and officers on data protection obligations;

- Monitoring compliance with data protection legislation and this policy;
- Providing advice on Data Protection Impact Assessments (DPIAs);
- Acting as the primary contact point with the Information Commissioner's Office (ICO);
- Overseeing the handling of personal data breaches and data protection complaints.

5.3 Executive Management Team (EMT)

The Executive Management Team monitors compliance with data protection legislation through regular reports from the DPO and ensures that the Council has appropriate technical and organisational measures in place to protect personal data held by the Council.

5.4 Corporate Information Governance Group (CIGG)

The Council's corporate oversight group for information governance. The Director of Finance and Corporate Services Chairs the CIGG and will feed back to EMT any material concerns on information governance.

5.5 Assistant Directors and Lead Specialists

Assistant Directors and Lead Specialists are accountable for ensuring that processing activities within their service areas:

- Have a clearly identified lawful basis;
- Are covered by an appropriate privacy notice;
- Are accurately recorded in the Record of Processing Activities and Information Asset Register;
- Comply with this policy and all associated procedures and guidance.
- Report into the Corporate Information Governance Group whose remit extends beyond data protection but encompasses data protection

5.6 Officers and Members

All officers and elected Members must:

- Complete mandatory data protection training;
- Access personal data only where necessary for their role;
- Ensure personal data is kept secure; and
- Report any actual or suspected data protection breaches or concerns to the DPO immediately.

Access and use of personal data held by the Council is only permitted for the purpose of carrying out official duties. Use for any other purpose is prohibited. Deliberate

unauthorised access to, copying, destruction or alteration of or interference with any computer equipment or data is strictly forbidden.

The Council maintains a Record of Processing Activities in accordance with Article 30 of the UK GDPR. Assistant Directors and Lead Specialists are responsible for ensuring that processing activities within their service areas are accurate, complete and kept up to date.

Breaches of this policy by employees may be addressed in accordance with the Council's disciplinary procedures. Breaches by elected Members may be addressed under the Members' Code of Conduct.

---

6. Collection of Personal Data

When collecting personal data, officers must ensure that:

- Individuals are informed why the data is being collected and how it will be used;
- Only data that is necessary for the specified purpose is collected;
- An appropriate privacy notice is provided at the point of collection.

All forms, online services and data collection tools must include a short privacy statement and signpost individuals to the full privacy notice on the Council's website.

Where personal data relates to children, additional care will be taken to ensure processing is fair, transparent and appropriate, and that privacy information is provided in an age-appropriate manner where applicable.

Privacy notices must be reviewed and updated where processing activities, purposes, lawful bases or data sharing arrangements change, and must accurately reflect current processing practices.

---

7. Data Sharing and Disclosure

Personal data must not be shared internally or externally with third parties unless:

- There is a lawful basis for the disclosure; and
- The disclosure is covered by a privacy notice or a formal data sharing or data processing agreement.

Any processing performed by a third party on behalf of the Council must only be done in compliance with this policy and the Data Sharing and Disclosure Policy. The responsibility and liability for any processing undertaken by a third party rests with the Council as the data controller. Under no circumstances should third parties be

engaged to deliver services (no matter how trivial) involving personal data or information until and unless suitable data processing clauses are included in the contract covering the work or a separate data processing agreement has been signed. A template data processing agreement template can be found on the intranet under Information Management. Assistant Directors and Lead Specialists are responsible for ensuring that such agreements are in place prior to any processing beginning. Advice should be sought from legal Services where there is any uncertainty.

If the Council is sharing personal data on a regular basis or receiving data on a regular basis with external organisations for a common purpose then a data sharing agreement should be used. A template data sharing agreement template can be found on the intranet under Information Management. Assistant Directors and Lead Specialists are responsible for ensuring that such agreements are in place prior to any processing beginning. Advice should be sought from legal Services where there is any uncertainty.

Requests for personal data from the police or other agencies must be considered carefully. The officer disclosing the information must identify their lawful basis for the disclosure (see section 4 above) and record their decision. This should include a description of the information disclosed, the name of the person and organisation the information was disclosed to, the date, the reason for the disclosure and the lawful basis. Such requests must be logged with the Customer Services team on the Council's ESB system.

'Business As Usual' requests for personal data (i.e. Benefit enquiries, Council Tax account balance queries, etc.) do not require the Data Subject to complete a Subject Access Request form, but you should ensure you know who you are responding to.

When personal data is disclosed internally or externally, it must be disclosed in a secure manner. More information about how to disclose information securely can be obtained from the Council's Chief Information Officer. ICT also have an Information Management Security Policy which can be found on the intranet in the Information Management section.

Where there is any uncertainty, advice must be sought from the Data Protection Officer via Legal Services.

---

8. Individual Rights and Requests

8.1 Individual Rights

Individuals have the following rights under the UK GDPR:

- the right to be informed;
- the right of access;

- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object to processing; and
- the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects.

Individuals have rights under UK GDPR, including the right of access to their personal data, rectification and being able to object to direct marketing. There are now also additional rights to have personal data processed for restricted purposes and the right to transfer data/have it transferred to another data controller (data portability) and a new 'right to be forgotten'. This means data subjects will be able to request that their personal data is erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with the DPA and UK GDPR.

However, further retention of such data will be lawful in some cases where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims.

To strengthen the 'right to be forgotten' online, the DPA and UK GDPR requires that a data controller who has made the personal data public should inform other data controllers which are processing the data to erase any links to, or copies or replications of, that data.

8.2 Subject Access Requests

Individuals have rights under UK GDPR to access to their personal data held by the Council. There are no formal requirements for a valid request. A person can make a SAR verbally or in writing, including by social media. They can make it to any part of the Council, and they do not have to direct it to a specific person or contact point.

All Subject Access Requests (SARs) must:

- Be forwarded immediately to the Customer Services team to log the SAR on ESB and coordinate the response;
- Be handled promptly and lawfully;
- Not be delayed, obstructed, amended or destroyed.

Under no circumstances should information be deleted or altered because an access request has been received and this could constitute a criminal offence under section 173(3) of the DPA.

A SAR should only be responded to once we are satisfied that we know the requestor's identity and the information relates to the person in question. Requests for identification must be reasonable and proportionate and requested to confirm the identity of the requestor.

There is no charge for a Subject Access Request unless the reproduction of material is such that it would not be financially viable for the Council to absorb. In this case the cost of reproduction, reformatting or assembly of material can be passed on to the requester.

When responding to individual rights requests, the Council will consider the rights of third parties and apply any relevant exemptions or restrictions under data protection legislation where applicable. Information will be redacted where disclosure would adversely affect the rights and freedoms of others and it could be unreasonable to disclose the information without the consent of the third party and the third party has not given consent or it would be unreasonable to ask for their consent.

8.3 Automated Decision-Making and Profiling

The Council does not ordinarily make decisions based solely on automated processing.

Where automated decision-making is used, appropriate safeguards will be in place, including the right to obtain human intervention, express their view and contest the decision. A DPIA must be completed and the DPO consulted before any automated decision-making is used.

---

9. Data Security

All personal data must be protected through appropriate technical and organisational measures, in line with the Council's Information Security Policy.

Minimum requirements include:

- Secure storage of paper records;
- Password-protected systems and locked screens;
- Strong system access controls;
- Secure methods for transferring personal data;
- Encryption of portable medium (laptop, memory stick, DVD, etc.)
- Compliance with all Council ICT and information security controls.

Technical and organisational measures will be proportionate to the risks presented by the processing and will be reviewed periodically to ensure they remain effective.

9.1 International Transfers of Personal Data

Where personal data is transferred outside the United Kingdom, the Council will ensure that appropriate safeguards are in place in accordance with UK GDPR Chapter V, including adequacy regulations, International Data Transfer Agreements or other approved mechanisms.

---

10. Personal Data Breaches

All actual or suspected personal data breaches must be reported **immediately** to the relevant Assistant Director and the Data Protection Officer.

A breach reporting form, available on the intranet, must be completed and sent to Legal Services mailbox as soon as becoming aware of an actual or suspected breach.

The Data Protection Officer will:

- Assess the incident and associated risks;
- Determine whether notification to the ICO and/or affected individuals is required;
- Ensure statutory reporting timescales are met.

Breaches must be reported to the ICO within 72 hours where there is a risk to the rights and freedoms of individuals. Where there is a high risk to individuals, affected individuals must also be notified without undue delay. In these cases, the DPO will make the decision whether the ICO, and affected individuals, must be notified of the breach and is the Council's point of contact with the ICO.

Near-miss incidents and weaknesses in processes that could result in a personal data breach should also be reported, to allow remedial action and organisational learning.

The DPO will retain records of all reported data breaches and report these on a periodic basis to EMT.

---

11. ICO Notification

The Council is required as a data controller to register with the ICO. The Council also has a duty to notify the ICO on an annual basis, confirming the types of personal data it processes along with the reason for processing the data.

Employees must inform the DPO of any new types of personal data that are being processed or which will be processed in the future. This will be added to the corporate

Information Asset Register and may require a data protection impact assessment to be carried out prior to the new process being implemented.

---

12. Retention and Disposal

The Council holds a vast amount of personal information. The DPA/UK GDPR requires that we do not keep personal data for any longer than is necessary. Personal data must be retained only in accordance with the Council's Records Retention and Disposal Policy.

When personal data is no longer required, it must be disposed of securely and in line with approved disposal procedures. Paper can be disposed of by the confidential waste process. Advice must be sought from the Chief Information Officer/ICT with regards to the disposal of data on electronic media or equipment.

---

13. Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment must be completed where:

- New processing activities are introduced; or
- Existing processing is significantly changed; or
- Processing is likely to result in a high risk to individuals' rights and freedoms.

The Data Protection Officer must be consulted at an early stage. A template DPIA form can be found on the intranet and must be signed off by the DPO and ICT.

Assistant Directors/Lead Specialists must ensure their service area's Information Asset Register is updated following completion of a DPIA.

---

14. Data Protection Complaints

Individuals may complain to the Council if they believe their personal data has been handled inappropriately. The Council has a formal complaint process which can be accessed here Complaints Policy - Rushcliffe Borough Council. Complaints relating to breaches or infringements of the UK GDPR will be dealt with under the Council's formal policy.

All complaints will be acknowledged in accordance with the timescales in the Council's Complaints Policy (and in any event within 30 days of receipt) and investigated without undue delay in line with statutory requirements and relevant ICO guidance.

The Data Protection Officer will oversee the handling of data protection complaints and ensure that outcomes are communicated to the complainant.

Individuals retain the right to escalate their complaint to the Information Commissioner's Office if they remain dissatisfied with the outcome.

---

15. Training and Awareness

All officers and Members must complete mandatory data protection training as required. Refresher training will be provided periodically.

---

16. Related Policies and Guidance

This policy should be read alongside:

- Computer Usage Policy
- Data Privacy Impact Assessment Policy
- Data Sharing and Disclosure Policy
- DPA/UK GDPR Guidance on the intranet
- Encryption Policy
- Freedom of Information Policy and procedures;
- Use of Generative Artificial Intelligence (GenAI) Policy
- Incident Management Policy
- Information Classification Policy
- Information Security Policy
- Records Retention and Disposal Policy;
- Removable Media Policy; and
- Any relevant guidance or instruction issued by the DPO, Legal Services and ICT on relevant matters including, but not limited to, DPIA, IARs, breach reporting and the handling of SARs.

---

17. Review

This policy will be reviewed at least every three years, or earlier where there are changes to legislation, statutory guidance or Council processing activities and / or practices.