Rackheath Community Council Data Protection Policy

1. Introduction

Rackheath Community Council ("the Council") is committed to protecting the rights and privacy of individuals in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy sets out how the Council processes, stores, and protects personal data.

2. Scope

This policy applies to all personal data processed by the Council, including data relating to residents, staff, councillors, contractors, and service users, in both electronic and paper formats.

3. Data Protection Principles

The Council shall process personal data in accordance with the following principles:

- Lawfulness, fairness and transparency: Personal data must be processed lawfully, fairly and in a transparent manner.
- Purpose limitation: Data must be collected for specified, explicit and legitimate purposes.
- Data minimisation: Data collected must be adequate, relevant and limited to what is necessary.
- Accuracy: Data must be accurate and, where necessary, kept up to date.
- Storage limitation: Data must not be kept in an identifiable form longer than necessary.
  Integrity and confidentiality: Data must be processed securely, to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage.
- Accountability: The Council must be able to demonstrate compliance with these principles.

4. Lawful Basis for Processing

Processing of personal data is permitted where at least one lawful basis (Article 6, UK GDPR) applies, including:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Public task (exercising official authority)
- Legitimate interests (where applicable)

Special category data will only be processed under Article 9 bases and with additional safeguards.

5. Data Subject Rights

Individuals have the right to:

- Be informed about how their data is used
- Access their personal data
- Request rectification or erasure
- Restrict or object to processing
- Data portability (where applicable)
- Lodge a complaint with the Information Commissioner's Office (ICO)

The council's Subject Access Request procedure is stated at Annexe 2, and the Freedom of Information Request procedure at Annexe 3.

6. Data Security

The Council will:

- Use authority-owned email accounts for all official business
- Store data securely, with access limited to authorised personnel
- Regularly review and update security measures
- Ensure safe disposal of data and equipment

7. Data Breaches

All data breaches will be reported to the Clerk and recorded. Where required, breaches will be reported to the ICO in accordance with statutory requirements: see annex 1 for the Data Breach Policy.

8. Data Audits and Retention

The Council will conduct regular data audits to identify what personal data is held, how it is used, and ensure it is processed lawfully. Data will be retained only as long as necessary, in line with the Council's retention schedule.

9. Training and Awareness

All staff and councillors will receive regular training on data protection principles and practices.

10. Data Protection Officer

Under Section 7 of the Data Protection Act 2018, parish councils are exempt from the requirement to appoint a Data Protection Officer, but may do so voluntarily.

11. Privacy Notice

The Council will provide clear privacy notices informing individuals about how their data is used.

12. Review

This policy will be reviewed every two years or in response to changes in legislation or guidance.

For questions, requests or concerns relating to this policy contact:
The Clerk to Rackheath Community Council
The Pavilion, Green Lane West, Rackheath NR13 6LT
Email: clerk@rackheathparishcouncil.org.uk
Telephone: 01603 920990

Annexe 1

Rackheath Community Council Data Breach Policy

1. Purpose

To set out the Council's approach to recognising, reporting, managing, and recording all personal data breaches, ensuring compliance with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.

2. Scope

This policy applies to all Council members, employees, volunteers, and contractors who process personal data on behalf of the Council.

3. Definitions

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Procedure

4.1 Recognition

Any person who becomes aware of a possible data breach must report it immediately to the Clerk (Data Protection Officer if appointed).

4.2 Reporting

All suspected breaches must be reported without delay. Use the Council's reporting form and provide as many details as possible (date, nature, type of data, people affected, likely consequences).

4.3 Containment and Recovery

The Clerk will work with IT support or relevant contractors to contain the breach and recover data where possible. Where data is lost or compromised, steps must be taken to mitigate adverse effects.

4.4 Assessment

The Clerk will assess the risk to individuals and the Council. If there is a risk to individuals' rights or freedoms, the breach must be reported to the Information Commissioner's Office (ICO) within 72 hours.

4.5 Notification

Affected individuals must be informed if the breach is likely to result in a high risk to their rights and freedoms. The ICO will be notified where appropriate, including required details under the UK GDPR.

4.6 Record-Keeping

All breaches, regardless of severity, must be documented in the Council's Data Breach Log, including:

- Description of the breach
- Date and time discovered
- Persons involved
- Containment measures
- Outcome and lessons learned

Annexe 2

Rackheath Community Council Subject Access Request procedure

1. Purpose

To outline the process by which individuals may access personal data held about them by the Council in line with the UK GDPR ("Right of Access").

2. Scope

Applies to all Council staff, councillors, contractors and volunteers who may receive, process, or respond to SARs.

3. What is a Subject Access Request?

A SAR is a request from an individual (or a person authorised to act on their behalf) to receive:

- Confirmation whether the Council processes their personal data
- Access to that personal data
- Supplementary information about the Council's processing

SARs may be made verbally or in writing (including via email or social media). No specific form of words is required.

4. Procedure

4.1 Receipt and Acknowledgement

- All staff and councillors must forward SARs to the Clerk without delay.
- The Clerk will:
    - Log the SAR (including the date of the request and method by which it was received)
    - Acknowledge receipt to the requester within 5 working days, confirming the deadline for response

4.2 Identity Verification

- The Council may request proof of identity if the request is unclear or sensitive data is involved.

4.3 Locating Information

- The Clerk will coordinate searches for relevant information across records, emails, cloud storage, and paper files.

4.4 Review and Redaction

- The Clerk will review all data. The Council may redact or withhold information where legal exemptions apply (e.g., third party personal data).

4.5 Response

- The Council must respond “without undue delay” and within 1 calendar month of receipt (or, if identity verification required, after ID is provided).
- The response must:
    - Include a copy of the requested personal data
    - Explain the purposes, retention periods, and who data is shared with
    - Advise on the right to complain to the ICO if dissatisfied

4.6 Extensions and Complex Requests

- In complex cases, the Council may extend the deadline by up to two months— the applicant will be informed within the initial month, explaining the reason for the extension.

4.7 No Fee Principle

- SARs are generally free. A “reasonable fee” may be charged for manifestly unfounded, excessive, or repeat requests.

5. Records

All SARs received and handled must be logged, including outcomes and any correspondence.

Annexe 3

Rackheath Community Council Freedom of Information Request procedure

1. Purpose

To outline how FOI requests will be received, processed, and responded to, fulfilling the Council's statutory duties under the Freedom of Information Act 2000.

2. Scope

This procedure applies to all information held by the Council in any format, unless exempt under the Act.

3. Rights under FOIA

Anyone, anywhere, can request recorded information held by the Council. Requests may be made in writing (including email or social media, but NOT by telephone), must include the applicant's real name, and provide an address for correspondence.

4. Receipt and Logging

- FOI requests received by staff, councillors, or volunteers must be passed to the Clerk immediately.
- The Clerk will log each request, recording:
    - Date received
    - Applicant's name and contact details
    - Nature of the request

5. Acknowledgement

- The Clerk will acknowledge the request within 5 working days.
- If clarification is required, the Clerk will contact the applicant as soon as possible.

6. Response Timeline

- The Council must respond to valid requests within 20 working days of receipt or once any clarification is provided.
- If more time is needed to consider the public interest test, an extension may be applied per legislation and the applicant informed.

7. Gathering and Assessing Information

- The Clerk will coordinate to locate all relevant recorded information.
- Information will be assessed for possible exemptions (see section 9).

8. Disclosure

- Unless an exemption applies, the Clerk/RFO will provide the requested information in the format preferred by the applicant (where reasonably practicable).
- If the information cannot be released, the applicant must be told why and informed of the right to appeal.

9. Exemptions

- Some information may be withheld if an exemption applies (e.g., personal data, confidential, or commercially sensitive information; Section 21, 40, 41, etc. of FOIA).
- The reasons for any exemption must be explained to the applicant.

10. Fees

- The Council will not charge a fee unless the cost of compliance exceeds the "appropriate limit" set by regulations. Applicants will be notified if this applies.

11. Appeals and Complaints

- Applicants can request an internal review if dissatisfied. The council's review should be completed within 20 working days.
- Dissatisfied applicants may then complain to the Information Commissioner's Office (ICO).

12. Publication Scheme

- The Council will maintain and update its Publication Scheme, making information proactively available as required by FOI law.

13. Record Keeping

- The Clerk must keep a record of all FOI requests and responses for audit and learning purposes.