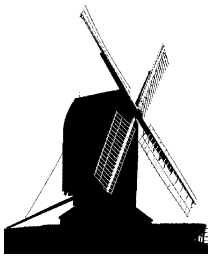

Rolvenden Parish Council

Data Protection Policy

Introduction

RolvendenParish Council ("the Council") is committed to complying with the UK General Data Protection Regulation ("UK-GDPR") and the Data Protection Act 2018 ("DPA 2018"), as amended by the Data (Use and Access) Act 2025 ("DUAA 2025").

The Council follows procedures intended to ensure that all personal data it collects about councillors, employees, residents, suppliers and others is processed fairly, lawfully and transparently.

Data protection law requires a balance between the Council's need to function effectively and respect for the rights and freedoms of individuals. This policy sets out how the Council intends to safeguard those rights and freedoms.

These obligations are mandatory rather than optional. The Information Commissioner's Office ("ICO") may impose penalties of up to £17.5 million or 4% of annual turnover, whichever is higher, for breaches of the data protection principles and individuals' rights, and up to £8.7 million or 2% of annual turnover for breaches of certain other obligations. In practice the ICO's approach to a council of this size would be proportionate, and its published position is that it prefers to work with public bodies to secure compliance rather than to fine them. The figures are given for completeness, not as an expectation.

Anyone permitted to access personal data in the course of their duties must comply with this policy and undertake any training appropriate to their role.

An individual who knowingly or recklessly obtains, discloses or retains personal data without the consent of the Council may commit a criminal offence under section 170 of the DPA 2018. Altering, defacing or destroying information to prevent disclosure following a request may be an offence under section 173. Employees may in addition be subject to the Council's disciplinary procedures.

Scope

This policy applies to the collection and processing of all personal data held by the Council in any format, including paper, electronic, audio and visual. It applies to all councillors, employees, volunteers and contractors.

Personal data and special category data

Personal data means any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Special category data means personal data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data, where processed to uniquely identify a person;
- data concerning health;
- data concerning a person's sex life or sexual orientation.

Except where stated otherwise, references in this policy to personal data include special category data.

Personal data relating to criminal convictions and offences is not special category data, but is subject to separate safeguards under Article 10 UK-GDPR and Schedule 1 DPA 2018. The Council must have both a lawful basis under Article 6 and an appropriate condition under Schedule 1 before processing such data.

Personal data processed by the Council

The Council processes personal data concerning its councillors, employees, residents, suppliers and others. The categories of data processed and the purposes for processing are described in the Council's privacy notice.

The Council maintains a record of its processing activities in accordance with Article 30 UK-GDPR. The exemption for organisations with fewer than 250 staff does not apply to the Council, because its processing of employee, councillor and correspondence records is regular rather than occasional. The record is maintained by the Clerk and reviewed annually.

The Data Controller

Rolvenden Parish Council is the Data Controller for all personal data relating to its councillors, employees, residents, suppliers and other individuals.

The Council is registered with the ICO as a fee payer. Its registration reference is ZB947259. The Council will maintain its registration and will keep its entry on the ICO register accurate and current.

Roles and responsibilities

The Clerk and Proper Officer

The Clerk and Proper Officer has day-to-day responsibility for ensuring that the Council complies with its data protection obligations and acts as the representative of the Data Controller.

Data Protection Officer

The Council is not required to appoint a statutory Data Protection Officer. Parish and town councils are excluded from the mandatory appointment requirement at Article 37(1)(a) UK-GDPR by virtue of the definition of "public authority" at section 7 DPA 2018.

Councillors

Councillors process personal data in two distinct capacities, and the distinction matters. When acting as a member of the Council (for example, sitting on a committee), the councillor processes data on behalf of the Council as controller.

All councillors and employees

All councillors and employees are responsible for collecting, storing and processing personal data in accordance with this policy, and for informing the Council of changes to their own personal data.

The Clerk should be contacted:

- with any question about the operation of this policy, data protection law, retention, or security;
- where there is a concern that this policy is not being followed;
- where it is unclear whether there is a lawful basis for a particular use of personal data;
- where consent needs to be relied on or captured;
- where a data subject seeks to exercise their rights;

- before personal data is transferred outside the United Kingdom;
- immediately, where a personal data breach is known or suspected;
- before a new activity begins that may affect the privacy of individuals;
- where personal data is to be shared with a third party, or a contract involving personal data is contemplated.

The data protection principles

Anyone processing personal data must comply with the principles at Article 5(1) UK-GDPR. Personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and, where necessary, kept up to date, with every reasonable step taken to erase or rectify inaccurate data without delay;
- kept in a form permitting identification of data subjects for no longer than is necessary for the purposes for which it is processed;
- processed in a manner ensuring appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Lawful basis for processing

The Council must identify a lawful basis under Article 6 UK-GDPR before processing personal data. Most of the Council's processing is carried out under Article 6(1)(e), the performance of a task carried out in the public interest or in the exercise of official authority, supported by the Council's statutory functions and section 111 of the Local Government Act 1972.

The Council may also rely on Article 6(1)(c) (legal obligation), Article 6(1)(b) (contract, for example in employment or supply arrangements), or Article 6(1)(a) (consent).

The Council does not generally rely on Article 6(1)(f), legitimate interests, because that basis is not available to public authorities for processing carried out in the performance of their tasks.

Where special category data is processed, an additional condition under Article 9 UK-GDPR is required, and in most cases a further condition under Schedule 1 DPA 2018 together with an Appropriate Policy Document.

Individuals' rights

The Council recognises the rights conferred on data subjects by the UK-GDPR:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure, where it applies;
- the right to restrict processing in certain circumstances;
- the right to data portability, where processing is based on consent or contract and carried out by automated means;
- the right to object to processing carried out under public task;
- rights relating to automated decision-making and profiling.

Not all rights are absolute. The right to erasure and the right to data portability, in particular, are of limited application to a council whose processing rests largely on public task.

The Council will respond to requests within one calendar month of receipt. This period may be extended by up to two further months where the request is complex or where a number of requests have been received from the same person, in which case the Council will inform the requester within the first month and explain the reason for the extension.

The Council may seek proof of identity, or clarification where the request is unclear and the Council processes a large quantity of data about the requester. Where the Council does so, the response period is paused until the information is received. The Council will not use identity or clarification requests to delay a response unnecessarily.

Requests should be made in writing to the Clerk at 5 Artisan Road, Headcorn, TN27 9AZ A request need not be in any particular form, need not mention data protection law, and need not be addressed to a particular person in order to be valid.

The Clerk must be informed of any request as soon as it is received. Exemptions from the duty to disclose exist in limited and specific circumstances and will be applied only where they properly apply, with the reasoning recorded.

A data subject dissatisfied with the Council's response may ask for the matter to be reviewed. An employee may seek resolution through the Council's grievance procedure. A data subject also has the right to complain to the ICO and to seek a judicial remedy.

Transparency

The Council publishes a privacy notice describing the personal data it processes, the purposes of that processing, the lawful bases relied on, retention periods, and how individuals may exercise their rights. The privacy notice is published on the Council's website and is kept current.

Data security

The Council has appropriate technical and organisational measures in place to protect personal data against unauthorised access, unauthorised or unlawful processing, and accidental loss, destruction or damage.

These measures include:

- technical controls appropriate to the nature of the data and the harm that might result from a breach;
- physical measures to protect Council premises and assets;
- checks on the reliability of persons with access to Council information;
- reporting and investigation of security incidents.

Detailed provisions on devices, passwords, encryption, removable media and remote working are set out in the Council's IT Policy and are not repeated here.

Material containing personal data that is no longer required, whether printed, handwritten or on electronic media, will be treated as confidential waste and disposed of securely.

Data processors

Where a third party processes personal data on the Council's behalf, the Council will appoint only processors providing sufficient guarantees that they will implement appropriate technical and organisational measures.

A written contract meeting the requirements of Article 28(3) UK-GDPR must be in place before processing begins. The Clerk is responsible for ensuring that such a contract exists and is retained.

The Council's processors currently include, but are not limited to, its website provider, its IT supplier and its payroll provider. The Clerk maintains a list of processors as part of the record of processing activities.

Sharing personal data

The Council does not routinely share personal data. It may do so where:

- there is a risk to the safety of Council staff or others;
- it is necessary to liaise with another agency;
- a supplier or contractor requires the data in order to provide a service to the Council.

The Council will also share personal data with law enforcement agencies, regulatory bodies and government departments where legally required or permitted, including for the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment or collection of tax, in connection with legal proceedings, or to discharge safeguarding obligations.

The Council may share personal data with the emergency services and other local authorities where necessary to respond to an emergency affecting any person.

Where the Council transfers personal data outside the United Kingdom, it will do so only where a valid transfer mechanism under Chapter V UK-GDPR applies. This includes transfers arising from the use of cloud services or website components hosted overseas, which are easily overlooked.

Monitoring of employees

Any monitoring of employees' use of Council systems will be proportionate to a specific and identified purpose, will be carried out in accordance with the ICO's guidance on employment practices and data protection, and will be preceded by a Data Protection Impact Assessment where the monitoring is systematic.

Employees will be informed of the nature and extent of any monitoring. Monitoring will not extend beyond what is necessary for the purpose identified, and information obtained through monitoring will be retained only for as long as that purpose requires.

The Council recognises that its capacity to monitor is not the same as an entitlement to do so, and that a monitoring regime broader than the Council's actual needs would be unlikely to satisfy Article 5(1)(c).

Data protection by design and by default

The Council will consider data protection at the outset of any new activity, system or process involving personal data, rather than after it has been implemented.

A Data Protection Impact Assessment is mandatory under Article 35 UK-GDPR where processing is likely to result in a high risk to individuals. For the Council, this is most likely to arise in relation to systematic monitoring of employees, surveillance of publicly accessible spaces, or the introduction of a new system processing personal data at scale. The Clerk must be consulted before any such activity begins.

Where a DPIA identifies a high risk that cannot be mitigated, the Council must consult the ICO before proceeding.

Retention

Personal data will be retained only for as long as necessary for the purpose for which it was collected. Retention periods are set out in the Council's retention schedule, which is maintained by the Clerk and reviewed annually.

Retention decisions take account of the Council's statutory obligations, the requirements of the Local Government Act 1972 in relation to minutes and statutory registers, limitation periods, and the public interest in the preservation of records of historical value.

Personal data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It includes accidental disclosure to the wrong recipient, loss or theft of a device or paper file, and inappropriate access to data.

Any known or suspected breach must be reported to the Clerk immediately, and in any event without delay. Individuals must not attempt to resolve a breach themselves before reporting it.

The Council will record every breach in an internal breach log in accordance with Article 33(5), whether or not it is reportable. The log records the facts, the effects, and the remedial action taken.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Council will report it to the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. The 72 hours runs from awareness, not from the start of the next working day, and includes weekends.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will also inform those individuals without undue delay.

Accountability

The Clerk is accountable for ensuring compliance with this policy and will report annually to the Council on data protection matters, including breaches recorded, rights requests received, and any outstanding risks.

The Council will keep its ICO registration current, maintain its record of processing activities, keep its privacy notice accurate, and assess the privacy impact of new or altered processing before it begins.