

UFFORD PARISH COUNCIL

Privacy Notice

For councillors, employees, applicants, volunteers, contractors and other role holders

Document status	Draft for Council review
Council approval	14/7/2026
Minute reference	14.07.26.9.b
Next review	July 2028, or sooner if legislation, guidance, services or processing arrangements change

1. Purpose of this notice

This notice explains how Ufford Parish Council collects, uses, stores, shares and protects personal data relating to councillors, employees, job applicants, volunteers, contractors, agents and other people carrying out roles for or on behalf of the Council. It is intended to meet the transparency requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Who is responsible for your data?

Ufford Parish Council is the data controller for the personal data covered by this notice. The Council determines why and how this information is used.

Data protection contact: the Clerk, Ufford Village Hall, Main Street, Ufford, Stamford PE9 3BH, email: clerk@ufford-pc.gov.uk.

Ufford Parish Council is enrolled in the CAPALC DPO Scheme and may seek data protection support through that scheme where appropriate. Data protection queries should be directed to the Clerk in the first instance.

Where appropriate, the Clerk may also seek advice from the Information Commissioner's Office, the Council's principal authority, the Council's professional advisers or relevant sector bodies.

3. Personal data covered by this notice

The Council may process the following categories of personal data, where relevant:

- name, title, address, telephone number, email address and other contact details;
- date of birth, national insurance number, tax code, pension information and payroll records;
- bank details, expenses, allowances, salary, payments and transaction records;
- employment, recruitment, right-to-work, qualification, training, appraisal and performance information;
- working pattern, absence, leave, sickness, occupational health and reasonable adjustment information;
- declarations of acceptance of office, registers of interests, gifts and hospitality, committee or representative roles and attendance records;
- correspondence, meeting records, complaints, grievance, disciplinary, investigation and legal records;
- images, photographs, website or social media references where relevant to Council business;
- system, device, email, website and security information where needed to protect Council systems and records;
- emergency contact and next-of-kin details; and
- any other information provided to the Council or generated while carrying out Council functions.

4. Special category and criminal offence data

Some information is more sensitive and receives extra protection under data protection law. The Council may process special category data, such as health information, disability information, equality monitoring data or trade union

information, only where it has both a UK GDPR Article 6 lawful basis and an Article 9 condition. Criminal offence data will only be processed where permitted by law and where necessary, for example in relation to recruitment, safeguarding, legal obligations or legal claims.

Where the Council relies on a Data Protection Act 2018 Schedule 1 condition that requires an Appropriate Policy Document, the Council should maintain that document separately from this privacy notice.

5. Where the Council obtains personal data from

- you directly, including forms, emails, applications, declarations, expense claims and correspondence;
- other councillors, employees, complainants, residents, contractors or meeting attendees;
- Peterborough City Council, HMRC, pension providers, payroll providers, insurers, auditors, banks, professional advisers and other public bodies;
- publicly available sources, where relevant to Council business; and
- Council systems, records, minutes, agendas, email accounts, website and IT arrangements.

6. Why the Council uses personal data and lawful basis

Purpose	Examples of personal data used	Main lawful basis under UK GDPR
Recruitment and appointment	Applications, CVs, interview notes, references, right-to-work checks, eligibility information	Article 6(1)(b) contract or steps before contract; Article 6(1)(c) legal obligation; Article 6(1)(e) public task where linked to public functions
Employment, payroll and pension administration	Salary, tax, NI, bank details, pension, expenses, leave, sickness and employment records	Article 6(1)(b) contract; Article 6(1)(c) legal obligation. Special category data may rely on Article 9(2)(b) employment and social security obligations
Councillor administration and democratic governance	Acceptance of office, attendance, register of interests, gifts and hospitality, representative roles, training records	Article 6(1)(c) legal obligation; Article 6(1)(e) public task/exercise of official authority
Meeting administration, decision-making and transparency	Agendas, minutes, reports, declarations of interest, correspondence and decisions	Article 6(1)(c) legal obligation; Article 6(1)(e) public task/exercise of official authority
Complaints, investigations, grievance, disciplinary and standards matters	Correspondence, witness evidence, investigation records, advice and outcome records	Article 6(1)(c) legal obligation; Article 6(1)(b) contract for employment matters; Article 6(1)(e) public task. Special category or criminal offence data may rely on Article 9/10 conditions where applicable
Health, safety, welfare and reasonable adjustments	Emergency contacts, accident reports, health information, disability information and adjustment requests	Article 6(1)(c) legal obligation; Article 6(1)(b) contract. Special category data may rely on Article 9(2)(b), Article 9(2)(f) legal claims or Article 9(2)(g) substantial public interest where applicable
Finance, audit, insurance and legal claims	Payment records, invoices, payroll records, audit evidence, insurance and legal correspondence	Article 6(1)(c) legal obligation; Article 6(1)(e) public task; Article 6(1)(b) contract where relevant
IT, security and records management	Email records, access records, device information and security incident records	Article 6(1)(c) legal obligation; Article 6(1)(e) public task; Article 6(1)(f) legitimate interests only where processing is outside public task functions

7. Key legislation and statutory functions

The Council may process personal data under, or in connection with, legislation and duties including the Local Government Act 1972, Localism Act 2011, Local Audit and Accountability Act 2014, Accounts and Audit Regulations 2015, Freedom of Information Act 2000, Environmental Information Regulations 2004, UK GDPR, Data Protection Act 2018, Equality Act 2010, Employment Rights Act 1996, Health and Safety at Work etc. Act 1974, PAYE and tax legislation, pension legislation, and other legislation relevant to parish council functions.

8. Sharing personal data

The Council will share personal data only where necessary and lawful. Recipients may include:

- Peterborough City Council, including elections, monitoring officer, planning, highways or other relevant services;
- HMRC, payroll provider, pension provider, bank, auditor, insurer and professional advisers;
- other public authorities, law enforcement bodies, courts or tribunals where required or permitted by law;
- contractors, service providers and IT providers acting under appropriate instructions or their own statutory responsibilities;
- the public, where information is lawfully published in agendas, minutes, registers, notices or the Council website; and
- other parties where required for legal claims, safeguarding, investigation, audit, transparency or statutory purposes.

9. Publication of councillor information

This privacy notice should be read alongside the Council's Data Protection Policy, Retention Schedule / Records Management Policy and Publication Scheme / Information Guide. The Publication Scheme explains what Council information is routinely published or made available under freedom of information requirements.

Some councillor information is published or made available because the law requires public accountability and transparency. This may include councillor names, roles, meeting attendance, registers of interests, declarations at meetings, decisions, minutes and certain contact details. Where a councillor has a sensitive interest, the Council will follow the statutory process for withholding sensitive details where the Monitoring Officer agrees.

10. How long the Council keeps personal data

The Council keeps personal data only for as long as needed for the purpose for which it was collected, including legal, audit, insurance, employment, tax, transparency, historical and archival requirements. Some records, such as minutes and key governance records, may be kept permanently. Financial and payroll records are usually retained for at least six years, and longer where required for audit, tax, pension, insurance or legal reasons. Recruitment records for unsuccessful candidates are normally kept for a limited period unless a longer period is justified.

The Council should maintain a separate retention schedule or records management policy setting out more detailed retention periods.

11. Security

The Council uses proportionate technical and organisational measures to protect personal data from unauthorised access, loss, misuse, alteration or disclosure. Measures include controlled access to electronic records, password protection, secure storage, use of official Council systems where available, careful publication checks and breach reporting arrangements.

12. International transfers

The Council does not routinely transfer personal data outside the UK. Some systems or website services may involve storage or access outside the UK. Where this occurs, the Council will take steps to ensure appropriate safeguards are in place, such as UK adequacy regulations, approved contractual safeguards or other lawful transfer mechanisms.

13. Automated decision-making

The Council does not make decisions about councillors, employees, applicants or role holders based solely on automated processing that produces legal or similarly significant effects.

Your data protection rights

Subject to the conditions and exemptions in data protection law, you may have the following rights:

- to be informed about how your personal data is used;
- to request access to your personal data;
- to ask for inaccurate or incomplete data to be corrected;
- to ask for personal data to be erased where there is no lawful reason for the Council to keep it;
- to ask for processing to be restricted in certain circumstances;
- to object to processing where the Council relies on public task or legitimate interests, although the Council may continue processing where it has compelling lawful grounds;
- to data portability, where this applies;
- to withdraw consent where consent is the lawful basis for processing; and
- to complain to the Information Commissioner's Office.

Requests should be sent to the Clerk. The Council may need to confirm your identity before responding. The Council will normally respond to subject access requests within one month, unless an extension is permitted by law.

Contact and complaints

Questions about this notice or requests to exercise data protection rights should be sent to the Clerk, Ufford Village Hall, Main Street, Ufford, Stamford PE9 3BH, email: clerk@ufford-pc.gov.uk.

You may also complain to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, telephone 0303 123 1113, or via www.ico.org.uk.

Review

This notice will be reviewed annually, or sooner if legislation, ICO guidance, Council services, suppliers, systems or processing arrangements change.