

UFFORD PARISH COUNCIL

General Privacy Notice

For residents, members of the public, correspondents, service users and meeting attendees

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 residents, members of the public, correspondents, complainants, meeting attendees, volunteers, grant applicants, service users, contractors and others who contact or interact with 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.

3. Personal data covered by this notice

Depending on the reason for contact with the Council, the Council may process:

- name, title, address, telephone number, email address and other contact details;
- correspondence, enquiries, complaints, comments, consultation responses and service requests;
- meeting attendance, public participation records, declarations or representations made to the Council;
- information about property, land, planning, highways, local amenities, parish assets or local services where relevant to the matter raised;
- grant, donation, payment, invoice, bank or transaction information where relevant;
- photographs, video or audio recordings where relevant and lawful, including events, assets, incidents or public meetings;
- website, email, social media and communication records;
- accident, incident, safeguarding, insurance or legal claim information; and
- any other information you provide to the Council or which is generated through Council business.

4. Special category and criminal offence data

The Council does not usually need special category data from residents or members of the public. However, it may sometimes process information such as health, disability, vulnerability, safeguarding or equality information where it is necessary to handle a request, make reasonable adjustments, respond to an incident, manage a complaint, administer a service, protect someone from harm, or deal with legal claims. Criminal offence data will only be processed where permitted by law and necessary for Council functions, safeguarding, complaints, incident management, fraud prevention 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 emails, letters, telephone calls, forms, meeting contributions and social media messages;
- other residents, councillors, employees, contractors, community organisations or public bodies;
- Peterborough City Council, police, emergency services, auditors, insurers, professional advisers and other public authorities;
- publicly available sources, including planning portals, public registers and websites, where relevant; and
- Council records, meeting papers, photographs, asset inspections and website/social media systems.

6. Why the Council uses personal data and lawful basis

Purpose	Examples of personal data used	Main lawful basis under UK GDPR
Responding to enquiries, correspondence and service requests	Contact details, correspondence, location or issue details	Article 6(1)(e) public task/exercise of official authority; Article 6(1)(c) legal obligation where applicable
Council meetings, public participation and democratic decision-making	Names, comments, representations, meeting records, agendas and minutes	Article 6(1)(c) legal obligation; Article 6(1)(e) public task/exercise of official authority
Planning, highways, parish assets and local services	Correspondence, property or location information, representations, photographs and site information	Article 6(1)(e) public task/exercise of official authority; Article 6(1)(c) legal obligation where applicable
Complaints, disputes, investigations and legal claims	Correspondence, evidence, witness information, incident records and advice	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. Special category data may rely on Article 9(2)(f) legal claims or Article 9(2)(g) substantial public interest where applicable
Finance, grants, contracts and payments	Invoices, bank details, payment records, grant applications and supplier details	Article 6(1)(b) contract; Article 6(1)(c) legal obligation; Article 6(1)(e) public task
Events, consultations and community engagement	Contact details, consultation responses, attendance information, photographs where appropriate	Article 6(1)(e) public task; Article 6(1)(a) consent where consent is appropriate, for example optional mailing lists or non-essential photography
Health, safety, safeguarding, insurance and incident management	Accident reports, incident details, health or vulnerability information, witness details and photographs	Article 6(1)(c) legal obligation; Article 6(1)(e) public task. Special category data may rely on Article 9(2)(c) vital interests, Article 9(2)(f) legal claims or Article 9(2)(g) substantial public interest where applicable
Website, records management and information rights	Website messages, email records, FOI/EIR/SAR records and publication evidence	Article 6(1)(c) legal obligation; Article 6(1)(e) public task

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, Health and Safety at Work etc. Act 1974, Occupiers' Liability legislation, planning and highways 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 planning, elections, highways, environmental services, monitoring officer or complaints teams;
- police, emergency services, safeguarding bodies or other public authorities where required or appropriate;
- contractors, suppliers, insurers, auditors, banks, payroll/finance providers and professional advisers;
- community organisations or event partners where necessary and lawful;
- the public, where information is lawfully included in agendas, minutes, reports, notices, registers or the Council website; and
- courts, tribunals or other bodies where needed for legal claims, audit, investigation or statutory compliance.

9. Publication and public meetings

The Council is required to conduct much of its business openly. Agendas, minutes and some supporting papers are published or made available to the public. Personal data will only be included where necessary and lawful. Members of the public who speak or submit written representations should be aware that their comments may be summarised in minutes or considered by councillors as part of Council business.

The Council will take care not to publish unnecessary personal data, confidential information or special category data. Where information is exempt or confidential, it may be withheld from publication or considered in private session where the legal requirements are met.

10. Photographs, recordings and social media

The Council may use photographs or recordings for lawful Council purposes, such as asset records, incident evidence, event publicity, website news or social media. Consent will be used where appropriate, particularly for close-up images of individuals or optional publicity. The Council will avoid publishing photographs of children or vulnerable individuals without appropriate consent unless there is a clear lawful reason.

11. 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, transparency, historical and archival requirements. Some records, such as minutes and key governance records, may be kept permanently. Financial records are usually retained for at least six years, and longer where required for audit, tax, insurance or legal reasons. Routine correspondence is retained only as long as it remains relevant to Council business.

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

12. 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 records, password protection, secure storage, use of official Council systems where available, careful publication checks and breach reporting arrangements.

13. International transfers

The Council does not routinely transfer personal data outside the UK. Some systems, website services or social media platforms 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.

14. Automated decision-making

The Council does not make decisions about residents or members of the public 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.