



EDINGTON PARISH COUNCIL GDPR PRIVACY NOTICE

GDPR Privacy Notice Update Timeline

- **Version:** 1.0
- **Adopted:** 14 September 2026
- **Adopted by:** Full Council
- **Published:** 14 September 2026
- **Review Due:** Feb/March 2027

Table of Contents

<i>Privacy Notice Update Timeline</i>	1
OVERVIEW	3
1. DATA PROTECTION OFFICER	3
2. DATA PROTECTION LEAD	3
3. PERSONAL DATA WE COLLECT	4
4. HOW WE USE DATA	4
5. LAWFUL BASIS FOR PROCESSING	5
6. DATA PROTECTION PRINCIPLES	5
7. DATA SHARING, STORAGE AND SECURITY	6
8. PRIVACY BY DESIGN AND DEFAULT	6
9. DATA AUDIT AND REGISTER	7
10. DATA RETENTION	7
11. DATA SUBJECT RIGHTS	7
12. MONITORING, CONTACT AND COMPLAINTS	8
ANNEX A - DEFINITIONS	9

OVERVIEW

Edington Parish Council is regulated in its use of Personal Data under the Data Protection Act 2018 and the General Data Protection Regulation. As a small parish council, we act as a corporate data controller under this legislation. This means that we decide how personal data is processed, and for what purposes. We are registered with the Information Commissioner's Office (ICO) as a 'Provider of council services' with the following registration details:

Edington Parish Council

Registration Reference: **ZA294198**

Date Registered: **8 January 2018**

Registration Expiry: **7 January 2027**

This policy sets out how the Parish Council seeks to protect Personal Data and ensure that councillors and the Clerk understand the rules governing its use. It applies to all councillors and staff and should be read in conjunction with the Parish Council's IT Policy. Annex A provides a list of key definitions of terms used in this legislation as they apply to this policy.

1. DATA PROTECTION OFFICER

Under section 7(3) of the Data Protection Act 2018, parish councils are not treated as 'public authorities' for UK GDPR purposes, so the Council is not automatically required to formally appoint a Data Protection Officer (DPO) on that basis. A DPO would still be required if the Council's core activities involved large-scale, regular and systematic monitoring of individuals, or large-scale processing of special category data — which they do not. As such, the Parish Council has not appointed a DPO.

2. DATA PROTECTION LEAD

Edington Parish Council, as a corporate body, is the Data Controller for the purposes of the Data Protection Legislation. Our Parish Clerk is our Data Protection Lead and has overall responsibility for the day-to-day implementation of this policy in respect to managing data protection compliance and how we collect, store, and handle personal data on the Council's behalf. To ensure that relevant compliance steps are addressed, the Clerk is required to consider data protection legislation and best practice before any significant new data processing activity is initiated.

Responsibilities of the Data Protection Lead

- Keeping the Council updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Assisting with data protection training and advice for all staff members and those included in this policy.
- Answering questions on data protection from staff, council members and other stakeholders.
- Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them.
- Checking and approving with third parties that handle the council's data contracts or agreement regarding data processing.

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Researching third-party services, such as cloud services the Council is considering using to store or process data.
- Approving data protection queries from residents, service users or media outlets.
- Liaising with external advisers, where needed, to ensure council communications and initiatives adhere to data protection law and this policy.

3. PERSONAL DATA WE COLLECT

The Parish Council holds Personal Data about its councillors, employees, residents, suppliers, and other individuals, for a variety of council purposes. We are committed to protecting privacy and processing personal data fairly and lawfully.

The Parish Council receives letters, phone calls and emails from people and organisations in relation to Parish matters or for consideration at Parish Council meetings. We may collect, store, and use the following types of personal data about residents, contractors, and visitors:

- **Contact details:** Names, titles, physical addresses, telephone numbers, and email addresses.
- **Financial data:** Bank account details (if we make payments to you or receive payments such as for burial plot purchases).
- **Asset management details:** Names, family lineage tracking, and ownership records linked to the parish burial ground.
- **Subscription data:** Email addresses and communication preferences for our digital newsletter.
- **Correspondence:** Information included in any letters, emails, or public comments sent to the council.

4. HOW WE USE DATA

We use personal data for purposes including, but not limited to:

- Managing the parish burial ground, including maintaining statutory burial records.
- Maintaining public safety and managing maintenance operations for the playfield and other assets such as the bus shelter.
- Distributing our monthly digital newsletter to subscribers.
- Managing parish council meetings, public consultations, and planning applications.
- Responding to enquiries, complaints, or requests for information.

5. LAWFUL BASIS FOR PROCESSING

We only process personal data when we have a legal reason to do so. Most commonly, we rely on:

- **Public Task:** Processing is necessary to perform duties as a local authority, such as maintaining our playfield and other assets for public safety and utility.
- **Contractual:** Processing is necessary in relation to a contract the data subject has entered into or wishes to enter into.
- **Legal Obligation:** Processing is necessary to comply with statutory duties other than contractual, e.g. the Local Authorities' Cemeteries Order 1977 for maintaining exclusive rights of burial and statutory burial registers.
- **Legitimate Interest:** Processing is necessary for the organisation's legitimate interest or those of a third party to whom the personal data is disclosed, except where such interests are overridden by the interests, rights or freedoms of the data subject.
- **Consent:** Clear consent has been given to process data for a specific purpose, such as opting into our monthly digital newsletter. Consent can be withdrawn at any time.

Where we process special category data (for example, information about religious denomination that may be recorded in connection with burial rites), we will also identify a specific condition under Article 9 of the UK GDPR, such as substantial public interest or explicit consent, before doing so.

6. DATA PROTECTION PRINCIPLES

The Parish Council will process personal data in compliance with the data protection principles of:

- **Lawfulness, fairness and transparency:** We will make sure that our data collection practices don't break the law and that we aren't hiding anything from data subjects.
- **Purpose limitation:** We will only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.
- **Data minimisation:** We will only process the personal data that we need to achieve our processing purposes.
- **Accuracy:** We will take all reasonable steps to erase or rectify data that is inaccurate or incomplete.
- **Storage limitation:** We will delete personal data when it is no longer necessary.
- **Integrity and confidentiality:** We will ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
- **Accountability:** We will take responsibility for how we process personal data, keep records to demonstrate our compliance, and review this policy and our data protection practices on a regular basis.

7. DATA SHARING, STORAGE AND SECURITY

Personal data will be treated as strictly confidential. We will only share it with third parties if required by law (such as reporting burial records), to prevent fraud, or with explicit consent (such as utilising a third-party email platform to distribute our newsletter). Where any third-party service we use to process personal data stores or processes data outside the UK, we will ensure an appropriate safeguard is in place, such as reliance on an applicable adequacy decision or standard contractual clauses.

We implement secure physical and electronic storage measures to protect data. Council staff and councillors will use official email addresses to ensure communication security.

The personal information (e.g. name, address, phone numbers and email addresses) will not be divulged to a third-party without the consent of the individual concerned other than for the purpose of dealing with them.

The Parish Council will ensure that any personal data it processes is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. The Parish Council will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. A data subject may ask for inaccurate personal data relating to them to be corrected.

Councillors must take reasonable steps to ensure that personal data the Parish Council holds about them is accurate and updated as required.

Personal data must be kept secure against loss or misuse. Where other organisations process personal data as a service on the Parish Council's behalf, the Clerk will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations. More specifically:

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it.
- Printed data will be shredded when it is no longer needed.
- Data stored on a computer will be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks will be similarly password protected.
- The Clerk must approve any cloud-based data storage.
- Data will be regularly backed up in line with the council's backup procedures.
- Data must never be saved directly onto unprotected mobile devices such as tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software and strong firewalls.

8. PRIVACY BY DESIGN AND DEFAULT

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Clerk will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan. When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

9. DATA AUDIT AND REGISTER

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. All Councillors and members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Parish Council to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

10. DATA RETENTION

We will keep personal data for no longer than is necessary. We follow statutory retention guidelines for local authorities:

- **Burial registers and plot allocations:** Kept indefinitely as required by UK law.
- **Minutes of meetings:** Kept indefinitely for historical archive.
- **Financial records:** Kept for 6 years plus the current financial year.
- **Newsletter subscription lists:** Kept until subjects choose to unsubscribe or withdraw consent.
- **General correspondence:** Kept for up to 2 years, or until the matter is resolved.

11. DATA SUBJECT RIGHTS

Under UK GDPR, a Data Subject is entitled, subject to certain exceptions, to request access to information held about them in a structured format. All Subject Access Requests must immediately be referred to the Clerk, who will respond within one calendar month of receipt. This period may be extended by up to two further months where a request is complex or numerous, in which case we will explain why the extension is needed. Responding to a request will not compromise the privacy of other individuals. A Data Subject may also request that their data is transferred directly to another system. Requests are usually dealt with free of charge, save in limited circumstances (such as manifestly unfounded or excessive requests) where we may charge a reasonable fee or decline to act.

Data Subjects may:

- **Access:** Request a copy of their personal data.
- **Correction:** Ask us to change or complete any inaccurate data.
- **Erasure:** Request that any information held on them is deleted or removed where it is no longer legally required, and any third parties who process or use that data must also comply with that request. An erasure request can only be refused if an exemption applies.
- **Restriction:** Ask us to limit how we use their data in certain scenarios.
- **Withdraw Consent:** Unsubscribe from our digital newsletter at any time.

12. MONITORING, CONTACT AND COMPLAINTS

The Council as a corporate body has ultimate responsibility for compliance. The Clerk will regularly monitor council activities and this policy to ensure adherence. If there are any questions or concerns about anything in this policy, do not hesitate to contact the Clerk.

To exercise your rights, raise a query, or make a complaint, please contact the Parish Clerk, Mr Malcolm Wieck, at:

- **Email:** clerk@edingtonwiltsparishcouncil.gov.uk
- **Address:** Sandy Lane Cottage, 12 Westbury Road, Edington, Westbury, Wiltshire, BA13 4QD
- **Phone:** 01380 830256

If you remain unsatisfied with our response, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

ANNEX A - DEFINITIONS

The General Data Protection Regulation “The GDPR” Regulation (EU) 2016/679 of the European Parliament and the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The Data Protection Legislation The Data Protection Act 2018 and the GDPR.

Personal Data Any information relating to an identified or identifiable living individual.

Data Subject An individual about whom personal data is held. It does not include anyone who has died, or who cannot be identified or distinguished from others.

Processing Data Processing in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as:

- collection, recording, organisation, structuring or storage,
- adaptation or alteration,
- retrieval, consultation, or use,
- disclosure by transmission, dissemination or otherwise making available,
- alignment or combination, or
- restriction, erasure, or destruction

Data Protection Officer Data Protection Legislation requires certain public authorities and data processors to appoint a Data Protection Officer (DPO). The role of the DPO is to assist the monitoring of internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for Data Subjects and the Supervisory Authority.

Data Controller Person or body that determines the purpose and means of the processing of Personal Data.

Sensitive Personal Data Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data, or of biometric data, for the purpose of uniquely identifying an individual; data concerning health; or data concerning an individual's sex life or sexual orientation. Data relating to criminal offences will be treated as Sensitive Personal Data.

Council Purposes The purposes of which Personal Data may be used by the Parish Council. Council purposes include the following:

- Compliance with legal, regulatory, and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests.
- Ensuring council policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, securing vetting and checking.
- The management and operation of the Council's cemetery, CCTV and allotments.
- Investigating complaints
- Ensuring safe working practices, general administration, payroll, providing access to systems and facilities.