ISLIP PARISH COUNCIL

DATA PROTECTION POLICY

Adopted by Council:	Islip Parish Council
Date Adopted:	March 2026 **(Minute 101/25)**
Review Date:	March 2027
Responsible Officer:	Parish Clerk
Contact:	clerk@islipparishcouncil.gov.uk

1. Introduction

Islip Parish Council (the Council) is committed to protecting the personal data it holds in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This policy sets out how the Council collects, uses, stores and protects personal data and the responsibilities of all councillors and the Clerk in doing so.

The Council is registered as a Data Controller with the Information Commissioner's Office (ICO). All data processing activities are carried out in accordance with the six principles of data protection.

2. Scope

This policy applies to all personal data processed by the Council, including data held in electronic and manual formats. It applies to all councillors, the Clerk, and any other person acting on behalf of the Council.

3. Data Protection Principles

The Council will ensure that all personal data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary for the purpose
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

4. Lawful Basis for Processing

The Council will only process personal data where it has a lawful basis for doing so. The lawful bases most commonly relied upon by the Council are:

- Legal obligation - where processing is necessary to comply with a legal requirement
- Public task - where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority
- Legitimate interests - where processing is necessary for the Council's legitimate interests, provided these are not overridden by the interests or rights of the data subject
- Contract - where processing is necessary for the performance of a contract with the data subject
- Consent - where the data subject has given clear consent for a specific purpose

5. Types of Personal Data Held

The Council holds personal data relating to the following categories of individuals:

5.1 Councillors and Officers

- Names, contact details and register of interests
- Correspondence and meeting papers
- Clerk employment records including payroll, HMRC records and appraisal records

5.2 Residents and Members of the Public

- Correspondence and representations submitted to the Council
- Planning application representations
- Contact details provided for council services or consultations

5.3 Service Users

- Allotment tenant details including name, contact details and tenancy records
- Burial ground records including names of the deceased, next of kin and contact details

5.4 Contractors and Suppliers

- Contact details and contractual information for contractors and service providers

6. Data Security

The Council will take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. These measures include:

- Use of the council's authority-owned email domain (clerk@islipparishcouncil.gov.uk) for all official communications
- Password protection of all electronic devices and accounts
- Secure storage of paper records
- Restricting access to personal data to those who need it for their role
- Ensuring personal data is not shared with third parties without a lawful basis

7. Data Retention

Personal data will be retained only for as long as is necessary for the purpose for which it was collected, in accordance with the Council's Document Retention and Disposal Policy (adopted October 2025). When data is no longer required it will be securely deleted or destroyed.

8. Data Breaches

In the event of a personal data breach, the Council will assess the risk to individuals and, where the breach is likely to result in a risk to their rights and freedoms, will notify the ICO within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to individuals, affected data subjects will also be notified.

Any suspected data breach must be reported to the Clerk immediately.

9. Rights of Data Subjects

Individuals have the following rights in relation to their personal data held by the Council:

- The right to be informed about how their data is used
- The right of access to their personal data (Subject Access Request)
- The right to rectification of inaccurate data
- The right to erasure in certain circumstances
- The right to restrict processing in certain circumstances
- The right to object to processing

Requests to exercise these rights should be made in writing to the Clerk at clerk@islipparishcouncil.gov.uk. The Council will respond within one month of receipt of the request.

10. ICO Registration

Islip Parish Council is registered with the Information Commissioner's Office as a Data Controller and pays the annual data protection fee. Registration details are available from the Clerk.

11. Record of Processing Activities (Data Map)

The Council maintains a Record of Processing Activities (Article 30, UK GDPR) — also referred to as a data map — which sets out all the personal data the Council processes, the purposes for which it is processed, the lawful basis relied upon, how it is stored, and how long it is retained. This document is maintained by the Clerk and is available to the ICO on request. All other data protection policies and the Council's Privacy Notice are based on and consistent with this record. The data map must be reviewed and updated whenever the Council's processing activities change.

12. Special Category Data

The Council may process special category personal data in certain circumstances, including health information relating to the Clerk's employment (for example, sickness absence records or reasonable adjustments) and, where relevant, information about the health of individuals in the context of burial ground records or other council services.

Special category data will only be processed where both a lawful basis and an additional condition under Schedule 1 of the Data Protection Act 2018 applies. Where the Council relies on the employment condition or the substantial public interest condition, it will maintain an Appropriate Policy Document (APD) as required by the DPA 2018. The APD will be held on file by the Clerk from before the processing commences and for a minimum of six months after processing ceases, and will be made available to the ICO on request.

13. Data Sharing

The Council will only share personal data with third parties where there is a lawful basis for doing so. Third parties with whom data may be shared include HMRC, the Council's bank, external auditors, contractors carrying out work on behalf of the Council, and other public authorities where required by law.

Where the Council engages a third party to process data on its behalf (a data processor), it will ensure that an appropriate written contract is in place which requires the processor to act only on the Council's instructions and to maintain appropriate security measures. Personal data will not be transferred outside the UK without appropriate safeguards in place.

14. Data Protection Impact Assessments

The Council will carry out a Data Protection Impact Assessment (DPIA) before commencing any new processing activity that is likely to result in a high risk to individuals, or where the nature, scope or purpose of existing processing changes significantly. A DPIA will always be considered when undertaking a new project involving personal data, introducing new technology, or sharing data in a new way. DPIAs will be documented and reviewed by the

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

15. Subject Access Requests

Any individual (a data subject) has the right to request access to the personal data the Council holds about them. This is known as a Subject Access Request (SAR). A SAR does not need to use prescribed wording — any written request asking what data the Council holds about an individual will be treated as a SAR.

The Clerk is responsible for managing all SARs. On receipt of a SAR, the Clerk will: acknowledge receipt promptly; begin a thorough search of all locations where council data is held (including email, Google Drive, paper records and, where applicable, councillors' personal devices used for council business); assess whether any exemptions apply; redact third-party data appropriately; and respond within one calendar month of receipt. The response must include the personal data itself and the supplementary information required by the UK GDPR (purposes, categories of data, recipients, retention periods, rights, and the right to complain to the ICO). If in doubt, advice should be sought from OALC or the Council's data protection adviser at the earliest opportunity.

16. Councillors as Data Controllers

This policy governs personal data for which the Council is the Data Controller. Councillors must be aware, however, that in some circumstances they may themselves act as a separate Data Controller — for example, where a resident contacts a councillor directly using the councillor's personal email address in their capacity as a local representative. Data received in this way is controlled by the individual councillor, not the Council, and must be kept entirely separate from council data. Councillors who act as Data Controllers in their own right are individually responsible for complying with the UK GDPR in respect of that data.

All personal data received by a councillor in connection with council business — including data sent to councillors by the Clerk — remains subject to this policy and the Council's IT Policy. Councillors must not use personal email accounts for council business, and must not forward or store council data on personal cloud storage platforms.

17. Training

The Clerk will undertake appropriate data protection training and keep up to date with changes in data protection law and guidance. The Council recognises that all councillors also have data protection obligations and will ensure that councillors have access to appropriate training to enable them to fulfil those obligations. This is particularly important where the Council undertakes projects involving significant processing of personal data, such as a Neighbourhood Plan. Training records will be maintained by the Clerk.

18. Responsibility and Review

The Clerk is responsible for ensuring compliance with this policy and for maintaining awareness among councillors of their data protection obligations. This policy will be reviewed annually and following any significant changes in data protection legislation or guidance.

19. Further Information

For further information about how the Council processes personal data, or to exercise your data subject rights, please contact:

The Parish Clerk

Islip Parish Council

Email: clerk@islipparishcouncil.gov.uk

For independent advice on data protection, contact the Information Commissioner's Office (ICO) at www.ico.org.uk or on 0303 123 1113.