Data Protection Policy

Little Longstone Parish Meeting

Version 1.0 – Approved at the assembly held on 26th August 2026

How to use this policy: *This is the Parish Meeting's internal operational policy for managing personal information and complying with data protection law. It sets out responsibilities, record-keeping, security, data sharing, breach management and the handling of data protection rights requests. It should be read alongside the Parish Meeting's Privacy Policy and Records Retention Policy.*

1. Purpose and scope

1.1 This policy sets out how Little Longstone Parish Meeting manages personal information and meets its obligations as a data controller under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.2 It applies to the Clerk, Chair, Vice Chair and anyone else handling personal information on behalf of the Parish Meeting.

1.3 This policy is the internal operational counterpart to the Parish Meeting's Privacy Policy, which explains to individuals how their personal information is used and their rights under data protection law.

2. Data controller status

2.1 Little Longstone Parish Meeting is the data controller responsible for personal information processed in connection with its functions. The Parish Meeting is registered with the Information Commissioner's Office (ICO) as a data controller under registration reference **ZC188583**.

2.2 The Parish Meeting is not required to appoint a Data Protection Officer (DPO). The Clerk is the principal contact for data protection matters.

3. Roles and responsibilities

3.1 The Parish Meeting is responsible for ensuring that appropriate arrangements are in place for compliance with data protection law.

3.2 The Clerk has day-to-day responsibility for data protection administration, including maintaining appropriate records of processing, handling data protection rights requests, managing the Parish Meeting's ICO registration and coordinating the response to personal data breaches.

3.3 The Chair works with the Clerk where a personal data breach, complaint or other significant data protection matter requires assessment or action.

3.4 Anyone handling personal information on behalf of the Parish Meeting must comply with this policy, the Privacy Policy and the Parish Meeting's security and records-management arrangements, and must report any suspected personal data breach promptly to the Clerk.

4. Data protection principles

4.1 Personal information must be:

- **processed lawfully, fairly and transparently;**
- **collected for specified, explicit and legitimate purposes** and not used incompatibly with those purposes;
- **adequate, relevant and limited** to what is necessary;
- **accurate and, where necessary, kept up to date;**

- **kept for no longer than necessary**, subject to the Parish Meeting's Records Retention Policy and lawful permanent preservation of records;
- **kept secure**, using appropriate technical and organisational measures.

4.2 The Parish Meeting is responsible for complying with these principles and must be able to demonstrate that compliance.

4.3 The Clerk will periodically review the personal information held by the Parish Meeting, the purposes for which it is used, the lawful basis for processing it, where it is held and who has access to it. The record of processing activities in section 5 will be updated where necessary following that review.

5. Record of processing activities

5.1 The Parish Meeting maintains the following record of its principal personal-data processing activities. The record should be reviewed periodically and updated when the Parish Meeting begins a significant new type of processing or materially changes an existing one.

Processing activity	Personal Information	Purpose	Lawful basis	Access / recipients	Retention
Correspondence and enquiries	Name, address, contact details and correspondence, including comments, enquiries and representations	Responding to correspondence and carrying out the Parish Meeting's public functions	Public task – Article 6(1)(e)	Clerk and others where necessary for the matter; relevant public authorities, advisers or other recipients where lawful and necessary	In accordance with the Records Retention Policy
Handling complaints	Names, contact details, complaint, correspondence, evidence and records of consideration and outcome	Handling complaints and maintaining effective governance	Public task – Article 6(1)(e)	Clerk, Chair or others involved in handling the complaint; advisers or other bodies where necessary and lawful	In accordance with the Records Retention Policy
Administration and recording of Parish Meeting governance	Names, contact details where required, attendance, decisions, declarations of interests and information relating to roles undertaken on behalf of the Parish Meeting	Conducting and recording Parish Meeting business and maintaining governance records	Public task – Article 6(1)(e); legal obligation – Article 6(1)(c), where applicable	Clerk and those involved in governance; information may be published or disclosed where required or appropriate	In accordance with the Records Retention Policy; some governance records are permanent
Administration of the Clerk's appointment	Contact details, employment or engagement records, payroll and payment information, correspondence and other records necessary to administer the role	Administering the Clerk's appointment, remuneration and applicable legal obligations	Contract – Article 6(1)(b); legal obligation – Article 6(1)(c)	Appropriate Parish Meeting office-holders; payroll, HMRC, pension or professional advisers where applicable	In accordance with the Records Retention Policy

Processing activity	Personal Information	Purpose	Lawful basis	Access / recipients	Retention
Banking, payments and financial controls	Names, contact details, signatures where required, banking-authorisation information and records of payments, approvals or checks	Managing and safeguarding public money and maintaining proper financial records	Legal obligation – Article 6(1)(c); public task – Article 6(1)(e)	Clerk, authorised office-holders or electors undertaking financial checks; banks, auditors and other bodies where necessary	In accordance with the Records Retention Policy
Tendering, award and administration of licences and other commercial arrangements	Names, business contact details, tender submissions, quotations or offers, financial information, licence or other commercial documentation, correspondence and payment information	Conducting competitive tender or other selection processes; awarding and administering licences and other commercial arrangements; and managing Parish Meeting assets and income	Public task – Article 6(1)(e); contract – Article 6(1)(b), where processing is necessary in relation to a contract or proposed contract with the individual	Clerk and those authorised to participate in the tender, selection, decision or administration; professional advisers and other recipients where necessary and lawful	In accordance with the Records Retention Policy; records of enduring legal, evidential or historical value may be retained permanently
Procurement of goods, services and professional advice	Names, business contact details, quotations, engagement or contractual records, correspondence, invoices and payment information	Obtaining goods, services and professional advice, selecting suppliers and advisers, administering contracts or engagements and making payment.	Contract – Article 6(1)(b), where applicable; legal obligation – Article 6(1)(c); public task – Article 6(1)(e)	Clerk and relevant Parish Meeting participants; banks, auditors and other appropriate recipients	In accordance with the Records Retention Policy
Legal, property and other official matters	Names, addresses, contact details, correspondence and other information relevant to the matter	Carrying out the Parish Meeting's functions, managing its land, assets and rights, protecting its legal interests and dealing with legal or administrative proceedings	Public task – Article 6(1)(e); legal obligation – Article 6(1)(c), where applicable	Clerk, relevant Parish Meeting participants, professional advisers, courts, public authorities and other recipients where necessary and lawful	In accordance with the Records Retention Policy; records of enduring legal or evidential value may be retained permanently
FOIA, EIR and data-protection rights requests	Name, contact details, request and correspondence, information necessary to verify identity where required, and the Parish Meeting's response	Responding to statutory information and data-protection requests and demonstrating compliance	Legal obligation – Article 6(1)(c)	Clerk; advisers or relevant bodies where necessary	In accordance with the Records Retention Policy

Processing activity	Personal Information	Purpose	Lawful basis	Access / recipients	Retention
Data-protection compliance and breach management	Details necessary to record, investigate and manage data-protection incidents or compliance matters	Preventing, investigating and responding to personal-data breaches and demonstrating compliance with data-protection law	Legal obligation – Article 6(1)(c)	Clerk, Chair where necessary, ICO, affected individuals, advisers or other bodies where required	In accordance with the Records Retention Policy

5.2 The Parish Meeting does not routinely seek to process special category personal data or criminal-offence data. Where such information is received or its processing becomes necessary, the Clerk must consider whether the information is necessary and identify the applicable lawful basis and any additional condition or legal authority required by data protection law before it is intentionally retained or otherwise processed.

5.3 Personal information which is not necessary for the purpose for which it was received should not be retained merely because it has been provided. Where appropriate, unnecessary information should be deleted, redacted or excluded from the relevant record, subject to the Records Retention Policy and any legal or evidential requirement to preserve the record.

6. Data Protection Impact Assessments

6.1 Before introducing new or significantly changed processing of personal information, the Clerk will consider whether a Data Protection Impact Assessment (DPIA) is required.

6.2 A DPIA must be carried out where proposed processing is likely to result in a high risk to the rights and freedoms of individuals. It may also be used where it would assist the Parish Meeting in identifying and reducing data-protection risks even if it is not legally required.

6.3 A DPIA will describe the proposed processing and its purpose, assess its necessity and proportionality, identify risks to individuals, and record the measures proposed to reduce those risks.

6.4 Where a DPIA identifies a high residual risk which cannot reasonably be reduced, the Parish Meeting will seek appropriate advice and, where required by law, consult the Information Commissioner's Office before the processing begins.

7. Data sharing and third parties

7.1 Personal information must not be shared with another person or organisation unless there is a lawful and necessary reason for doing so. Only the information reasonably required for the purpose should be shared, and appropriate security measures must be used when it is transmitted.

7.2 Where personal information is shared with another organisation which determines its own purposes and means of processing, that organisation will normally be an independent data controller. Examples may include public authorities, auditors, insurers, professional advisers and regulatory bodies. The Clerk should ensure that there is an appropriate lawful basis for the disclosure and that only necessary information is shared.

7.3 Where another organisation processes personal information on behalf of the Parish Meeting and only on its instructions, it is a data processor. Before such processing begins, the Clerk must ensure that an appropriate written contract or other binding arrangement containing the data-protection provisions required by law is in place.

7.4 Before engaging a new supplier or service provider which will have access to personal information, the Clerk should establish whether it will act as a processor or an independent controller and record the position where appropriate. Where it is a processor, appropriate data-protection and security arrangements must be in place before personal information is provided.

7.5 Where an office-holder, elector or other person is given access to personal information in order to carry out an authorised task on behalf of the Parish Meeting, access must be limited to what is necessary for that task. The information must be handled securely, used only for the authorised purpose and returned or securely deleted when access is no longer required.

7.6 Before personal information is included in an agenda, minute, report, website publication or other publicly available record, the Clerk should consider whether publication is necessary, lawful and proportionate. Personal information which does not need to be published should be omitted or redacted where appropriate.

8. Personal data breaches

8.1 A personal data breach is a security incident resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. This may include information being lost, sent to the wrong person, accessed without authority or otherwise compromised.

8.2 Anyone who becomes aware of a suspected or actual personal data breach must report it to the Clerk without undue delay. If the Clerk becomes aware of a breach, or the breach involves the Clerk, the Chair should also be informed where appropriate.

8.3 The Clerk will take prompt action to contain the breach where possible and will assess its nature, the personal information and individuals affected, the likely consequences, and the measures required to reduce the risk of harm.

8.4 All actual personal data breaches will be recorded. Suspected breaches should also be documented sufficiently to record their assessment and outcome where appropriate. The record should include the nature of the breach, its likely effects, the action taken, whether notification to the Information Commissioner's Office or affected individuals was required, and any measures taken to prevent recurrence.

8.5 Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Parish Meeting will notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If notification is made later than 72 hours, the reasons for the delay will be recorded.

8.6 Where a personal data breach is likely to result in a high risk to the rights and freedoms of an individual, the Parish Meeting will inform the affected individual without undue delay, unless data protection law provides that notification is not required.

8.7 Following a breach, the Clerk will consider whether changes are required to procedures, security arrangements, training, contracts or other controls in order to reduce the risk of recurrence.

9. Data subject rights requests

9.1 The rights available to individuals are summarised in the Privacy Policy. This section sets out the internal procedure for recognising and handling requests to exercise those rights.

9.2 A request does not need to use particular wording or refer to data protection law. Anyone receiving a request which may involve the exercise of a data protection right should pass it to the Clerk promptly. The Clerk will record the date received and identify which right or rights are being exercised.

9.3 The Clerk may ask for information reasonably necessary to confirm the requester's identity where this is not already clear. Where necessary, the Clerk may also ask the requester to clarify the information or processing to which the request relates. Only information reasonably necessary for these purposes should be requested.

9.4 The Clerk will identify and locate relevant records and consider what action the applicable right requires. Where information is to be disclosed, the Clerk must consider whether it also contains personal information about another individual, legally privileged material, confidential information or other information to which an exemption or restriction may apply.

9.5 Requests must be dealt with without undue delay and normally within one month of receipt. Where data protection law permits the response period to be extended, the requester must be informed within the initial one-month period and told the reason for the extension.

9.6 No fee will normally be charged for dealing with a request. A fee may be charged, or a request refused, only where data protection law permits this. The Clerk should obtain appropriate advice before refusing a request or charging a fee on this basis.

9.7 The response will explain the action taken. Where a request is refused or cannot be complied with in full, the requester will be given the reasons and informed of any applicable right to complain to the Information Commissioner's Office. The request, searches undertaken, decision and response should be recorded sufficiently to demonstrate compliance.

9.8 Where a request also engages the Freedom of Information Act 2000 or Environmental Information Regulations 2004, the Clerk should consider the applicable regimes together. The same information may require separate consideration under data protection and information-access legislation.

10. Training and awareness

10.1 The Clerk, Chair, Vice Chair and anyone else who is given access to personal information on behalf of the Parish Meeting should receive information, guidance or training appropriate to their role and the personal information they handle.

10.2 The Clerk will keep data protection requirements under review and obtain updated guidance or training where there are significant changes in legislation, regulatory guidance, Parish Meeting activities or the systems used to process personal information.

10.3 Anyone given temporary or occasional access to personal information for an authorised Parish Meeting purpose should be made aware of the need to keep the information secure, use it only for the authorised purpose and not disclose it inappropriately.

11. Security

11.1 The Parish Meeting will use appropriate technical and organisational measures to protect personal information against unauthorised or unlawful access, use, disclosure, alteration, loss or destruction. Security measures will be proportionate to the nature and sensitivity of the information and the risks arising from its processing.

11.2 Personal information should, so far as practicable, be held using Parish Meeting-controlled email, filing and storage arrangements rather than solely in personal accounts, files or equipment. Access should be limited to those who require it for an authorised purpose.

11.3 Electronic systems and accounts used to hold or access personal information should be protected by appropriate access controls, passwords and, where available and appropriate, multi-factor authentication. Devices and software should be maintained with appropriate security updates.

11.4 Important electronic records should be backed up or otherwise stored in a manner which provides appropriate protection against accidental loss and allows continuity of access if equipment, an account or an individual responsible for the records becomes unavailable.

11.5 Confidential or sensitive information should be transmitted and stored using security measures appropriate to the risk. Encryption or other additional safeguards should be used where appropriate.

11.6 Paper records containing personal information should be stored securely and should not be left accessible to people who do not have an authorised need to see them.

11.7 Personal information should not normally be stored permanently on personal devices or in personal email accounts. Where temporary use of a personal device or account is unavoidable, appropriate security must be maintained and the information should be transferred to the Parish Meeting's records and removed from the personal system when no longer required there.

11.8 Access to personal information should be removed promptly when an office-holder, contractor or other authorised person no longer requires it.

12. International transfers

12.1 Before using a service or arrangement which involves the transfer or processing of personal information outside the United Kingdom, the Clerk will establish whether the transfer is permitted under data protection law and whether any additional safeguards are required.

12.2 Where a supplier or data processor is used, the location of processing and any international transfers should be considered as part of the assessment and contractual arrangements required under section 7.

13. Resolution of adoption and review

13.1 This policy will be reviewed periodically and following any significant change in data protection law, regulatory guidance, the Parish Meeting's processing activities or the systems used to process personal information.

13.2 The record of processing activities in section 5 may be updated between formal policy reviews where necessary to reflect changes in processing, provided that any significant change in policy or governance arrangements is referred to the Parish Meeting for approval.

Date of policy: August 2026
Approving body: Little Longstone Parish Meeting
Date of Assembly and Minute Reference: 26th August 2026 – Minute reference 51/26
Policy version reference: 1.0
Policy effective from: 26th August 2026
Next review due: May 2027