Holme Low Parish Council

Data Protection Policy

1. Introduction

Holme Low Parish Council recognises its responsibility to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. These regulations set out high standards for the handling of personal information and protecting individuals' rights to privacy.

2. Digital Governance (Assertion 10 Compliance)

To comply with the requirements of the Practitioner's Guide 2025, the Council adheres to the following digital standards:

- **Official Email Accounts:** All Council business must be conducted using official email accounts on an authority-owned domain (e.g., @holmelow-pc.org.uk). The use of personal email accounts for Council business is strictly prohibited.
- **Data Audits:** The Council shall conduct a formal Annual Data Audit to identify what personal data is processed, the lawful basis for holding it, and to ensure its secure disposal.
- **Website Accessibility:** The Council will ensure its website meets WCAG 2.2 AA accessibility standards. The Clerk is responsible for ensuring the accessibility statement is reviewed and updated annually.
- **Cybersecurity:** Multi-Factor Authentication (MFA) must be enabled on all Council-domain accounts wherever the technology is supported.

3. Data Protection Principles

When dealing with personal data, Holme Low Parish Council staff and Members must ensure that data is:

- Processed fairly, lawfully, and transparently.
- Collected for specific, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Not kept longer than is necessary (refer to the Document Retention Policy).
- Processed in a manner that ensures appropriate security.

4. Roles and Responsibilities

The Council has appointed the Parish Clerk as the Data Protection Lead. The Lead is responsible for:

- Managing Subject Access Requests (SARs).
- Overseeing the annual data audit.
- Ensuring that all staff and Members receive regular training on data protection and cybersecurity best practices.

5. Rights of Individuals (Subject Access Requests)

Individuals have the right to access their personal data held by the Council.

- **Requests:** Must be made in writing to the Parish Clerk.
- **Fees:** Information will be provided free of charge unless the request is manifestly unfounded or excessive.
- **Timeline:** The Council must respond within one month of receiving the request.
- **Right to Erasure:** If an individual requests that their data be rectified or erased, the Council will comply unless there is a legal obligation to retain it.

6. Handling Information and Confidentiality

- **Members' Access:** If an elected Member needs to access information to carry out their duties, they may only access as much as is necessary for that specific purpose.
- **Consent:** Data should never be used for political reasons unless the data subjects have given explicit consent.
- **Breach Notification:** If a data breach is identified that poses a risk to individuals, the Information Commissioner's Office (ICO) must be informed within 72 hours.

7. Policy Review

This policy will be reviewed annually at the Annual Meeting of the Council to ensure compliance with emerging technology trends and audit requirements.

Adopted by the Parish Council	13 January 2026