

# Glanton Parish Council

## Data Protection and Privacy Policy

### **1. Purpose**

Glanton Parish Council is committed to protecting personal data and handling information lawfully, fairly and transparently in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and associated legislation.

The Council recognises that good data protection is an essential part of good governance and maintaining public trust.

### **2. Scope**

This policy applies to councillors, employees, contractors and volunteers acting on behalf of the Council, and all personal data processed by the Council.

This includes information held electronically, in paper form, photographs, audio recordings, emails, and other records created or received in connection with Council business.

### **3. Data Protection Principles**

The Council will ensure personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date where necessary
- Kept only for as long as necessary
- Stored securely and protected from unauthorised access, loss or disclosure
- Managed in a way that demonstrates accountability and compliance

### **4. Lawful Basis for Processing**

The Council will identify and record an appropriate lawful basis for all processing of personal data.

Common lawful bases used by the Council may include:

- Legal obligation
- Public task
- Contract
- Consent

Where the Council processes special category data, an additional lawful condition under Article 9 UK GDPR will also be identified.

## **5. Roles and Responsibilities**

The Council does not currently appoint a formal Data Protection Officer.

Responsibility for day-to-day data protection compliance rests with the Clerk, who acts as the Council's responsible officer for data protection matters.

Councillors and anyone acting on behalf of the Council must:

- Handle personal data responsibly and confidentially
- Only access personal data where necessary for Council business
- Not use personal data for personal, political or unrelated purposes
- Report any actual or suspected data breach immediately to the Clerk
- Follow this policy and associated procedures

## **6. Data Security**

The Council will take proportionate technical and organisational measures to protect personal data.

This may include:

- Password-protected devices and systems
- Secure cloud storage
- Multi-factor authentication where appropriate
- Locked storage for paper records
- Regular backups
- Restricted access to records
- Secure destruction of records when no longer required

## **7. Personal Devices and Email Use**

Councillors and staff using personal devices or personal email accounts for Council business must ensure appropriate security measures are in place.

Council information must:

- Be stored securely
- Not be shared inappropriately
- Be deleted when no longer required
- Only be accessed by authorised persons

## **8. Data Breaches**

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

The Council will investigate breaches promptly and determine whether notification to the Information Commissioner's Office (ICO) or affected individuals is required.

The Council will maintain records of data breaches where appropriate.

## **9. Individual Rights**

Individuals have the right to:

- Be informed about how their data is used
- Request access to their personal data
- Request correction of inaccurate data
- Request deletion of data in certain circumstances
- Restrict or object to processing
- Request transfer of data where applicable
- Complain to the Information Commissioner's Office (ICO)

Requests made under data protection legislation will normally be handled administratively by the Clerk in accordance with legal requirements.

## **10. Data Sharing**

Personal data will only be shared where lawful and necessary.

The Council may share information with government departments, regulatory bodies, auditors, professional advisers, contractors or service providers acting on behalf of the Council.

## **11. International Transfers and Cloud Services**

Some electronic systems or service providers used by the Council may store or process data outside the United Kingdom.

Where this occurs, the Council will seek to ensure appropriate safeguards are in place in accordance with UK GDPR requirements.

## **12. Retention and Disposal**

The Council will only retain personal data for as long as necessary for the purpose for which it was collected, or as required by law.

Records will be securely deleted, destroyed or archived in accordance with the Council's Retention Schedule.

## **13. Privacy by Design**

The Council will consider data protection implications when introducing new systems, services, projects or processes involving personal data.

Where appropriate, the Council may carry out a Data Protection Impact Assessment (DPIA).

#### **14. Freedom of Information**

Requests for information may also fall under the Freedom of Information Act 2000 or Environmental Information Regulations 2004 and will be handled in accordance with the relevant legislation.

#### **15. Training and Awareness**

Councillors and staff will be made aware of their responsibilities through induction, guidance and periodic training where appropriate.

#### **16. Review**

This policy will be reviewed every two years or sooner where required by changes in legislation, guidance or operational requirements.

### Part 2 – Privacy Notice

#### **17. Who We Are**

Glanton Parish Council is the data controller for the personal data it processes.

The Clerk is the main contact for data protection matters.

#### **18. What Personal Data We May Collect**

The Council may collect and process names, addresses, email addresses, telephone numbers, financial information where necessary, correspondence, photographs from public events, and information provided in applications, complaints or enquiries.

#### **19. Why We Process Personal Data**

The Council processes personal data in order to carry out its legal duties and functions, manage meetings and governance, administer finances and contracts, manage employment matters, respond to correspondence and enquiries, maintain records, deliver services and projects, and communicate with residents and stakeholders.

#### **20. Lawful Basis**

The Council processes personal data under one or more lawful bases including legal obligation, public task, contract, and consent.

Where consent is used, it may be withdrawn at any time.

#### **21. Sharing Information**

The Council does not sell personal data.

Information may be shared where necessary with councillors and employees, contractors or service providers, government bodies, auditors, professional advisers, and other public authorities where legally required.

## **22. Data Processors**

The Council may use external providers for services such as email hosting, website hosting, cloud storage, payroll and IT support.

Where providers process personal data on behalf of the Council, appropriate safeguards will be sought.

## **23. International Transfers**

Some providers used by the Council may store data outside the UK.

Where this occurs, the Council will seek to ensure appropriate safeguards are in place.

## **24. How Long We Keep Information**

Personal data is retained only for as long as necessary.

Retention periods are set out in the Council's Retention Schedule.

## **25. Your Rights**

You have the right to request access to your data, request correction of inaccurate data, request deletion in certain circumstances, object to processing, request restriction of processing, and lodge a complaint with the ICO.

## **26. Contact**

Questions relating to this policy or the Council's handling of personal data should be directed to the Clerk.

### **Appendix A – Retention Schedule**

This retention schedule sets out the minimum periods for which Glanton Parish Council will normally retain records and the method of disposal where appropriate.

Record Type	Retention Period	Reason / Authority	Disposal Method
Signed Council Minutes	Permanent	Legal and historical record	Archive
Draft Minutes	Until approved unless required for legal or complaint purposes	Administrative record	Delete
Agendas	3 years	Transparency and reference	Delete
Supporting Reports	6 years	Governance and audit trail	Secure deletion
Financial Records (invoices, receipts, bank statements)	6 years	HMRC requirement	Secure deletion/shredding
VAT Records	6 years	HMRC requirement	Secure deletion/shredding
Payroll Records	6 years	HMRC requirement	Secure deletion/shredding
Contracts and Agreements	6 years after expiry	Limitation Act 1980	Secure deletion/shredding
Asset Register	Permanent (current version retained)	Governance record	Archive superseded versions
Insurance Policies	6 years after expiry	Liability protection	Secure deletion
Routine Correspondence	12 months	Operational reference	Delete
Council Business Emails linked to decisions/contracts/complaints	Retain with relevant file	Governance and audit trail	Secure deletion
Complaint Files and Related Emails	6 years after closure	Governance and risk management	Secure deletion/shredding
Planning Correspondence	6 years minimum	Reference and audit trail	Secure deletion
FOI and SAR Requests	3 years after closure	Accountability record	Secure deletion
Superseded Policies	3 years after replacement	Governance record	Secure deletion
Safeguarding Incident Records	6 years	Risk management	Secure deletion
Website Contact Form Submissions	12 months unless part of formal record	Operational use	Delete

Records of historical significance may be retained permanently where appropriate.