EMERSONS GREEN TOWN COUNCIL

Data Protection Policy

Date approved: 18th June 2026

Approved by: Full Council

Next Review date: June 2029

Contents:

1. Introduction

Emersons Green Town Council holds personal data about employees, councillors, residents, suppliers, and other individuals for a variety of Council purposes. This policy sets out how the Council protects personal data and ensures compliance with the Data Protection Act 2018 and UK GDPR.
This policy combines general data protection requirements with specific procedures for handling data breaches.
This policy applies to all councillors, staff, and volunteers.

2. Definitions

Personal Data: Information relating to identifiable individuals.

Sensitive Personal Data: Data relating to race, health, political views, religion, criminal records, or similar.

Data Breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples:

- Lost or stolen devices
- Sending personal data to the wrong recipient
- Unauthorised access to systems
- Loss of access due to system failure or ransomware

3. Scope

This policy applies to all individuals who handle personal data on behalf of the Council.
The Clerk (Data Protection Officer) has overall responsibility for implementation and compliance.

4. Principles of Data Protection

The Council will ensure that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Stored securely
- Retained only as long as necessary

5. Responsibilities

Clerk / Data Protection Officer:

- Oversee compliance with GDPR and DPA
- Maintain records of processing activities
- Provide advice and training
- Conduct risk assessments and privacy impact assessments
- Manage data breaches and reporting

Council:

- Ensure policies and processes are in place
- Maintain a Privacy Notice
- Ensure lawful basis for processing

Councillors and Staff:

- Handle personal data securely
- Always follow this policy
- Report breaches promptly

6. Data Handling and Security

- Paper data must be stored securely and shredded when no longer needed
- Digital data must be password-protected
- Data should not be stored on unauthorised devices
- Approved cloud services must be used
- Regular backups must be performed
- Personal data must not be shared unnecessarily

7. Data Subject Rights

Individuals have the right to:

- Access their data (Subject Access Requests)
- Correct inaccurate data
- Request deletion (Right to be Forgotten)
- Receive their data (Data Portability)

Requests must be referred to the Clerk and responded to within one month.

8. Data Breach Management

Reporting:

- All breaches must be reported immediately to the Clerk
- A breach reporting form must be completed

Response:
The Clerk will:

- Assess the risk to individuals
- Contain and recover data where possible
- Record the breach in the register

Notification:

- ICO must be notified within 72 hours if there is risk
- Individuals must be informed if there is high risk

Review:
After each breach, the Council will:

- Review causes
- Assess response effectiveness
- Implement improvements

9. Monitoring and Training

- Staff must receive regular GDPR training
- Compliance will be monitored by the Clerk
- Audits will be conducted periodically

10. Consequences of Non-Compliance

Failure to comply with this policy may result in disciplinary action and potential legal consequences.

11. Data Audit and Register

The Council maintains a data register detailing:

- What data is held
- Where it is stored
- Who is responsible
- Retention periods

12. Monitoring and Review

This policy will be reviewed regularly and updated as required due to operational or legal changes.

The latest version will always be available on the Council website:
http://www.emersonsgreen-tc.gov.uk/council-policies-and-key-documents

13. Data Breach Reporting Form

To be completed immediately upon discovery of a breach.

Date and time of Notification of Breach	
Notification of Breach to whom – Name: Contact Details:	
Details of Breach -	
Nature and content of Data Involved -	
Number of individuals affected –	
Name of person investigating breach - Name: Job Title: Contact details: Email: Phone number: Address:	
The Information Commissioner Office informed - Time and method of contact: https://report.ico.org.uk/security-breach/	
Police Informed if relevant - Time and method of contact Name of person contacted Contact details	

Individuals contacted – How many individuals contacted? Method of contact used to contact?	
Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Staff briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	