

EAST GOSCOTE PARISH COUNCIL

DATA PROTECTION POLICY (INTERNAL GOVERNANCE DOCUMENT)



Approved by:	Full Council	Date: 21.9.26
Last reviewed:	September 2025	
Next review due:	September 2027	

Data Protection Policy

1. Policy Statement

East Goscote Parish Council is committed to protecting the privacy and personal information of residents, councillors, employees, volunteers, contractors, suppliers and all other individuals whose personal data it processes.

The Council recognises its responsibilities as a data controller under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and associated legislation. The Council will process personal data lawfully, fairly, transparently and securely and will ensure appropriate technical and organisational measures are in place to safeguard personal information.

This policy forms part of the Council's governance framework and applies to all councillors, employees, volunteers, contractors and anyone processing personal data on behalf of the Council.

2. Purpose

The purpose of this policy is to:

- demonstrate the Council's commitment to complying with data protection legislation;
- establish responsibilities for handling personal data;
- ensure personal information is processed consistently and securely;
- protect the rights and freedoms of individuals;
- reduce the risk of personal data breaches.

3. Scope

This policy applies to all personal data processed by the Council regardless of format, including:

- electronic records;
- paper records;
- emails;
- photographs;
- CCTV images (where applicable);
- audio recordings;
- information held by contractors acting on behalf of the Council.

4. Definitions

Personal Data

Any information relating to an identified or identifiable living individual.

Special Category Data

Personal data requiring additional protection, including information concerning health, racial or ethnic origin, religious beliefs, political opinions, trade union membership, genetics, biometrics, sex life or sexual orientation.

Processing

Any operation performed on personal data including collection, recording, storage, use, disclosure, amendment or destruction.

Data Subject

The individual to whom personal data relates.

5. Data Protection Principles

The Council will comply with the seven principles of UK GDPR by ensuring personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- retained only for as long as necessary;
- processed securely using appropriate technical and organisational measures;
- processed in a manner that demonstrates accountability.

6. Lawful Processing

The Council will only process personal data where a lawful basis exists.

The lawful basis will normally be one or more of the following:

- Legal obligation
- Public task
- Performance of a contract
- Consent
- Vital interests

Where special category data is processed, the Council will identify both a lawful basis and an appropriate condition under the Data Protection Act 2018.

7. Roles and Responsibilities

Full Council

The Council is ultimately responsible for ensuring that East Goscote Parish Council complies with the UK General Data Protection Regulation, the Data Protection Act 2018 and associated legislation. The Council will ensure that appropriate policies, procedures and resources are in place to support compliance.

Clerk and Data Protection Lead

The Parish Clerk acts as the Council's Data Protection Lead and is responsible for:

- monitoring compliance with data protection legislation;
- maintaining the Council's data protection documentation;
- maintaining the Record of Processing Activities;
- advising councillors and employees on data protection matters;
- responding to requests relating to personal data;
- managing data protection complaints;
- coordinating responses to personal data breaches;
- arranging appropriate training where required.

Councillors, Employees and Volunteers

Everyone processing personal information on behalf of the Council shares responsibility for protecting that information.

Individuals must:

- comply with this policy and all related procedures;
- only collect and use personal information where necessary for legitimate Council business;
- only access personal information that they are authorised to access;
- ensure personal information is accurate and kept up to date where they are responsible for maintaining it;
- keep personal information confidential;
- protect passwords and login credentials;
- lock computers or mobile devices when left unattended;
- store paper records securely;
- ensure confidential waste is disposed of securely;
- only transfer personal information using approved and secure methods;
- not store Council personal data on personal devices unless expressly authorised by the Clerk and appropriate security measures are in place;
- not disclose personal information to third parties unless authorised and there is a lawful basis to do so;
- report actual or suspected personal data breaches immediately to the Clerk;
- seek advice from the Clerk whenever they are unsure how personal information should be handled.

Anyone processing personal information on behalf of the Council remains responsible for maintaining confidentiality even after they cease to be employed by, or hold office within, the Council.

Failure to comply with this policy may result in disciplinary action, removal from authorised access to Council information, or other appropriate action depending on the circumstances.

8. Confidentiality

All councillors, employees, volunteers and contractors are expected to maintain the confidentiality of personal information obtained through their work with the Council.

Personal information must only be accessed where necessary for authorised Council business and must never be used for personal purposes or disclosed without appropriate authority.

Confidential information should be protected at all times by:

- restricting access to authorised individuals only;
- using strong passwords and secure authentication methods;
- locking devices when unattended;
- securing paper records in locked storage;
- avoiding unnecessary printing of personal information;
- ensuring confidential documents are not left unattended in public or shared spaces;
- verifying the identity of individuals before disclosing personal information;
- using secure methods when sending personal information electronically.

Council information must not be stored on personal devices or personal cloud storage services unless expressly authorised by the Clerk and appropriate security measures are in place.

Where home or remote working is undertaken, individuals must ensure that confidential information remains secure and is not accessible to family members, visitors or other unauthorised persons.

9. Information Security

The Council will implement appropriate technical and organisational measures to safeguard personal information.

These measures include, where appropriate:

- password-protected systems;
- multi-factor authentication where available;
- antivirus software and regular security updates;
- secure electronic storage;
- encryption where appropriate;
- restricted access based on business need;
- regular backups;
- secure destruction of confidential information;
- physical security for paper records and Council equipment.

The Council will regularly review its security arrangements to ensure they remain appropriate to the risks associated with its processing activities.

10. Data Sharing

The Council will only share personal information where:

- required by law;
- necessary to perform its public functions;
- required under a contract;
- consent has been obtained where appropriate.

Where external organisations process information on behalf of the Council, appropriate written agreements will be in place.

11. Individual Rights

Individuals have the right to:

- be informed about how their information is used;
- request access to their personal data;
- request correction of inaccurate information;
- request erasure where applicable;
- request restriction of processing;
- object to processing in certain circumstances;
- request data portability where applicable;
- withdraw consent where processing relies on consent.

Requests should be made to the Clerk.

The Council will normally respond within one calendar month.

12. Personal Data Breaches

All actual or suspected personal data breaches must be reported immediately to the Clerk.

The Council will:

- investigate all reported breaches;
- take immediate steps to contain the breach;
- assess risks to individuals;
- maintain a breach register;
- notify the Information Commissioner's Office where required;
- notify affected individuals where there is a high risk to their rights and freedoms.

The Council's detailed procedures are contained within the Data Breach Procedure.

13. Data Protection Complaints

Eligibility to Make a Data Protection Complaint

To make a data protection complaint, an individual must be directly affected by:

- The Council's use of their own personal data, or
- The Council's response to a data protection request they have made

Complaints cannot be made by individuals who are not personally impacted.

Council Complaints Procedure

If an individual wishes to complain about how their personal data has been handled, they should follow the Council's Complaints Procedure, which sets out:

- How to submit a complaint
- How the Council will investigate and respond
- Expected timescales
- How outcomes are communicated

The Clerk will signpost the individual to the Complaints Policy upon request.

Escalation to the Information Commissioner's Office (ICO)

If the individual remains dissatisfied after completing the Council's Complaints Procedure, they may escalate the matter to the Information Commissioner's Office (ICO):

- Website: www.ico.org.uk
- Telephone: 0303 123 1113

The ICO may investigate concerns about how personal data has been handled.

14. Training

The Council will ensure that councillors, employees and others handling personal information receive appropriate data protection awareness training and are informed of their responsibilities.

Additional training will be provided where roles involve regular processing of personal data.

15. Monitoring and Review

The Clerk will monitor compliance with this policy and report significant data protection issues to the Council where appropriate.

This policy will be reviewed annually, or sooner where required by changes in legislation, guidance or the Council's processing activities.

Related Documents

This policy should be read alongside the Council's:

- General Privacy Notice
- Data Breach Policy
- Record of Processing Activities (Article 30)
- Subject Access Request Policy
- Freedom of Information Policy
- IT Policy
- Complaints Procedure

Signed.....

(Chair)

Date.....