

Lostock Gralam Parish Council

Data Protection Policy

1. Introduction

Lostock Gralam Parish Council recognises that personal information must be collected, processed and stored responsibly.

This Data Protection Policy sets out how the Council complies with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Council is committed to ensuring that personal information is:

- processed lawfully, fairly and transparently;
- collected for specified purposes;
- limited to what is necessary;
- accurate and kept up to date;
- retained only for as long as necessary;
- kept securely.

2. Scope

This policy applies to all personal information processed by Lostock Gralam Parish Council.

It applies to:

- the Clerk and Responsible Financial Officer;
- Councillors;
- volunteers;
- contractors and service providers where applicable.

The policy covers information held in:

- electronic records;
- emails;
- documents;
- paper files;
- CCTV recordings;
- meeting records.

3. The Council's Responsibilities

Lostock Gralam Parish Council is the Data Controller for the personal information it processes.

The Council is responsible for ensuring that:

- appropriate procedures are in place;
- personal information is handled securely;
- individuals' rights are respected;
- data breaches are dealt with appropriately;
- staff and councillors understand their responsibilities.

The Clerk acts as the Council's main point of contact for data protection matters.

4. Data Protection Principles

The Council follows the seven principles of UK GDPR.

Lawfulness, fairness and transparency

The Council will only process personal information where there is a lawful basis for doing so and will explain how information is used.

Purpose limitation

Information will only be used for the purpose for which it was collected unless there is another lawful reason to use it.

Data minimisation

The Council will only collect information that is necessary.

Accuracy

The Council will take reasonable steps to ensure information is accurate and kept up to date.

Storage limitation

Information will not be kept for longer than necessary.

Security

The Council will protect personal information against unauthorised access, loss, damage or disclosure.

Accountability

The Council will maintain appropriate records and procedures to demonstrate compliance.

5. Responsibilities of Councillors

Councillors must:

- only use personal information obtained through Council duties for legitimate Council purposes;

- keep confidential information secure;
- not share personal information without authority or a lawful reason;
- use Council email accounts for Council business;
- report any suspected data breach to the Clerk promptly.

Councillors must take care when handling information received through their role, particularly where it relates to residents, complaints or sensitive matters.

6. Responsibilities of the Clerk

The Clerk is responsible for:

- maintaining Council records securely;
- ensuring appropriate retention and disposal of information;
- managing requests from individuals regarding their personal information;
- reporting and managing data breaches;
- ensuring suppliers and contractors handling personal data are appropriately managed;
- advising the Council on data protection matters.

7. Information Security Arrangements

The Council uses a range of measures to protect personal information.

These include:

- Council-owned computer equipment;
- Council email accounts;
- password protection;
- restricted access to Council documents;
- secure electronic storage;
- secure backup arrangements;
- secure disposal of confidential information.

Council documents are stored electronically using Microsoft OneDrive. Access is restricted to authorised Council personnel.

Important electronic records are backed up securely, with backup copies stored in a fire-resistant safe.

8. Use of Council Equipment

Council equipment must only be used for authorised Council purposes.

The Council laptop must:

- be protected by appropriate passwords;
- not be shared with unauthorised persons;
- be kept secure when not in use;
- have appropriate security updates applied.

Any loss, theft or suspected compromise of Council equipment must be reported immediately.

9. Email and Electronic Communications

The Council provides email addresses for Councillors and the Clerk for Council business.

Council email accounts should be used when communicating Council information.

Users must take care when sending emails containing personal information, including:

- checking recipients before sending;
- avoiding unnecessary disclosure of personal information;
- using appropriate methods when sharing confidential information.

The Council is working towards implementing .gov.uk email addresses as part of improving its digital governance arrangements.

10. CCTV

The Council operates CCTV at the Council-owned play area.

CCTV is used to:

- protect Council property;
- support public safety;
- assist with investigations where necessary.

CCTV footage:

- is stored locally;
- is automatically overwritten after approximately 30 days;
- is accessed only by authorised persons;
- is downloaded only where necessary, such as for police investigations or complaint investigations.

Further details are contained within the Council's CCTV Policy.

11. Data Processors and Third Parties

Where the Council uses external organisations to process personal information, reasonable steps will be taken to ensure that information is handled securely.

Examples include:

- DM Payroll Ltd for payroll processing;
- NEST for pension administration;
- website hosting providers;
- auditors;
- insurers;
- contractors where necessary.

The Council will only share information where there is a lawful basis to do so.

12. Data Breaches

A personal data breach occurs when personal information is:

- lost;
- accidentally disclosed;
- accessed without permission;
- altered without authorisation;
- destroyed incorrectly.

Examples include:

- sending information to the wrong person;
- losing paperwork;
- losing equipment containing Council information;
- unauthorised access to files.

All suspected breaches must be reported to the Clerk immediately.

Breaches will be assessed and managed in accordance with the Council's Data Breach Procedure.

Where required, the Information Commissioner's Office (ICO) will be notified within the required timescales.

13. Requests for Personal Information

Individuals have rights under UK GDPR, including the right to request access to their personal information.

The Council will manage requests in accordance with its Subject Access Request Procedure.

Requests should be directed to the Clerk.

14. Retention and Disposal

The Council will retain information only for as long as necessary.

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

When information is no longer required it will be securely destroyed or deleted.

15. Training and Awareness

The Council will ensure that those handling personal information understand their responsibilities.

Relevant training and guidance will be provided where appropriate.

16. Review of Policy

This policy will be reviewed regularly to ensure it remains effective and reflects changes in legislation, technology and Council working practices.

Document Version: 2

Date Adopted: September 2026

Review Date: September 2029

Responsible Officer: Clerk and Responsible Financial Officer