Langstone Community Council: Data Protection and GDPR Policy

Adopted: 10/02/2026

Review Date: 12/05/2026

Signed:

1. **Introduction**

Langstone Community Council ("the Council") is committed to protecting the rights and freedoms of individuals whose personal data it collects and processes. This policy sets out how the Council complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The Council recognises its responsibilities as a Data Controller and ensures that personal data is handled lawfully, fairly, transparently, and securely.

2. Scope

This policy applies to:

- All councillors
- All employees
- Volunteers, contractors, and anyone acting on behalf of the Council

It covers all personal data processed by the Council in any format (electronic, paper, audio, visual, or otherwise).

3. Key Definitions

- Personal Data: Any information relating to an identified or identifiable living individual.
- Special Category Data: Sensitive data requiring additional protection (e.g., health, ethnicity, political opinions).
- Processing: Any operation performed on personal data, including collection, storage, use, sharing, or deletion.
- Data Subject: The individual to whom the personal data relates.
- Data Controller: The organisation determining the purpose and means of processing personal data (Langstone Community Council).
- Data Processor: A third party processing data on behalf of the Council.

4. Data Protection Principles

The Council adheres to the seven principles of the UK GDPR:

Lawfulness, fairness, and transparency

1. Personal data must be processed lawfully, fairly, and in a transparent manner.

Purpose limitation

2. Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

Data minimisation

3. Data collected must be adequate, relevant, and limited to what is necessary.

Accuracy

4. Personal data must be accurate and kept up to date.

Storage limitation

5. Data must not be kept longer than necessary for the purposes for which it is processed.

Integrity and confidentiality (security)

6. Personal data must be processed securely, protecting against unauthorised access, loss, or damage.

Accountability

7. The Council must be able to demonstrate compliance with all principles.

5. Lawful Bases for Processing

The Council processes personal data under one or more lawful bases defined in Article 6 of the UK GDPR, including:

- Public task
- Legal obligation
- Contract
- Consent
- Vital interests
- Legitimate interests (rarely used by public authorities)

Special category data is processed only under Article 9 conditions, such as substantial public interest or explicit consent.

6. Rights of Data Subjects

Under the UK GDPR, individuals have the following rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making (not used by the Council)

Requests must be responded to within one month. The Council will not normally charge a fee.

7. Data Subject Access Requests (DSARs)

Individuals may request access to their personal data.

The Council will:

- Verify the identity of the requester
- Respond within one month
- Provide data in an intelligible, secure format
- Redact third-party information where necessary

Fees are only charged where requests are manifestly unfounded or excessive.

8. Data Security

The Council will implement appropriate technical and organisational measures, including:

- Password protection and access controls
- Secure storage of paper records
- Encryption where appropriate
- Shredding or secure disposal of confidential waste
- Regular data backups
- Staff training on data protection responsibilities

9. Data Breaches

A personal data breach is any incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The Council will:

- Record all breaches
- Assess risk to individuals
- Report notifiable breaches to the Information Commissioner's Office (ICO) within 72 hours
- Inform affected individuals where there is a high risk to their rights and freedoms

10. Data Sharing and Third Parties

The Council will only share personal data with:

- Organisations with a lawful basis for receiving it
- Processors who provide sufficient guarantees of compliance
- Statutory bodies where required by law

Data sharing agreements will be used where appropriate.

11. Retention and Disposal

The Council follows the Local Government Association / SLCC retention schedules.

Data will be:

- Kept only as long as necessary
- Reviewed regularly
- Disposed of securely

12. Training and Awareness

All councillors, employees, and volunteers handling personal data will receive appropriate training. Refresher training will be provided periodically.

13. Data Protection Officer (DPO)

Under the DPA 2018, community councils are not automatically required to appoint a DPO.

However, the Council will designate a responsible officer to oversee compliance and act as the point of contact for data protection matters.

14. Policy Review

This policy will be reviewed every two years or sooner if legislation or Council operations change.

Data Protection Policy Guidelines

1. Introduction

1.1 These guidelines expand on the Council's Data Protection Policy and should be read alongside it.
1.2 The UK GDPR and the Data Protection Act 2018 replaced the Data Protection Act 1998. They apply to all personal data held electronically or in structured paper filing systems.
1.3 The legislation reinforces the principles of confidentiality, accountability, and transparency.

1.4 These guidelines apply only to information relating to living individuals.

2. Responsibilities

2.1 The Council is the Data Controller and is responsible for ensuring compliance with data protection law.
2.2 A designated officer will oversee data protection compliance, maintain records of processing activities, and act as the point of contact for data protection matters.
2.3 All councillors, employees, and volunteers must follow the UK GDPR principles when processing personal data.
2.4 Any new system, process, or project involving personal data must undergo a Data Protection Impact Assessment (DPIA) where required.

2.5 Staff must report any actual or suspected data breach immediately so it can be assessed and, if necessary, reported to the ICO within 72 hours.

3. Data Collected and System Contents

3.1 Only the minimum personal data necessary for a specific purpose should be collected and retained.
3.2 Personal data must be relevant, accurate, and kept up to date. Inaccurate or outdated information must be corrected without delay.
3.3 Staff must not record unnecessary, subjective, or inappropriate comments in any system.

3.4 Special category data (e.g., health information) must only be processed where a lawful basis under Article 6 and a condition under Article 9 apply.

4. Collecting and Using Personal Data

4.1 When collecting personal data, individuals must be informed of:

- The purpose for which their data is being collected
- The lawful basis for processing
- Who it may be shared with
- How long it will be retained
- Their rights under the UK GDPR

This is normally provided through the Council's Privacy Notice.
4.2 Personal data must only be used for the purpose for which it was collected unless a new lawful basis applies and the individual has been informed.
4.3 Personal data must not be disclosed to third parties without a lawful basis or the individual's consent (unless required by law).

4.4 Staff must take care when responding to telephone or email enquiries to ensure the identity of the requester is verified.

5. Data Subject Rights and Access Requests

5.1 Individuals have rights under the UK GDPR, including access to their personal data, rectification, erasure (where applicable), restriction, and objection.

5.2 Data Subject Access Requests (DSARs):

- Must be acknowledged and completed within one month
- Cannot normally incur a fee
- Require identity verification

Must exclude or redact third-party information unless consent has been obtained

- 5.3 Systems must be designed so DSARs can be fulfilled efficiently and securely.

6. Security Measures

6.1 Appropriate technical and organisational measures must be in place, including:

- Password protection and access controls
- Secure storage of paper records
- Encryption where appropriate
- Regular backups

Secure disposal (e.g., shredding)

6.2 Personal data must only be accessed by individuals who have a legitimate need to do so.

- 6.3 Portable devices (laptops, USB drives) must be handled securely and not used to store personal data unless encrypted.

7. Data Sharing and Third Parties

7.1 Personal data may only be shared with third parties where:

- A lawful basis exists
- Sharing is necessary and proportionate

A written data processing agreement is in place (for processors)

- 7.2 Data must not be transferred outside the UK unless appropriate safeguards are in place.

8. Retention and Disposal

8.1 Personal data must be retained only for as long as necessary for the purpose for which it was collected.
8.2 The Council will follow its approved Retention Schedule.

8.3 Data must be disposed of securely to prevent unauthorised access.

9. Training and Awareness

9.1 All councillors, employees, and volunteers who handle personal data must receive data protection training.

9.2 Refresher training will be provided periodically or when legislation changes.

10. Disciplinary Action

10.1 Failure to comply with this policy and its guidelines may result in disciplinary action.

10.2 Individuals may also be personally liable under the Data Protection Act 2018 for unlawful handling of personal data.