Data Compliance and Information Security Policy

1. Introduction

North Marston Parish Council ("the Council") is committed to complying with all applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and related legislation. This policy sets out the Council's approach to managing personal data responsibly and securely.

2. Purpose

This policy aims to ensure that:

- Personal data is collected, stored, processed, and shared in compliance with legal requirements.
- The privacy rights of individuals are respected and protected.
- Appropriate security measures are in place to protect Council data, including email communications.
- Staff and councillors understand their responsibilities regarding data protection.

3. Scope

This policy applies to all personal data processed by the Council, whether in electronic or paper form, including data relating to residents, staff, councillors, contractors, and third parties.

4. Data Protection Principles

The Council will ensure that all 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.
- Kept only as long as necessary.
- Processed securely to protect against unauthorized or unlawful processing, accidental loss, destruction, or damage.

5. Roles and Responsibilities

- The Council's Data Protection Officer (DPO) is responsible for overseeing compliance and providing guidance.
- All councillors, staff, and contractors must comply with this policy and data protection laws.
- Breaches of this policy may lead to disciplinary action.

6. Use of Email and Communication Security

- To comply with recent government guidance and legislation, all official Council communications **must use secure email addresses**.
- Where possible, councillors and staff should use **gov.uk email addresses** for official correspondence to enhance security and public trust.
- Personal email addresses should **not** be used for official council business.
- Emails containing personal or sensitive data should be encrypted or sent through secure channels.
- Staff and councillors must be vigilant against phishing attempts, suspicious attachments, or links.

7. Data Storage and Security

- Personal data must be stored securely, with appropriate physical and technical safeguards.
- Access to personal data is restricted on a need-to-know basis.
- Passwords and access controls should be strong and regularly updated.
- Paper records must be kept in locked cabinets or secure areas.

8. Data Sharing

- Personal data will only be shared with third parties where there is a lawful basis and proper safeguards.
- Data sharing agreements must be in place where applicable.
- Requests for data from external parties (including the public and media) must follow the Council's Freedom of Information and Data Subject Access Request procedures.

9. Data Breach Management

- Any actual or suspected data breach must be reported immediately to the Clerk.
- The Council will assess the breach and take appropriate action, including notification to the Information Commissioner's Office (ICO) if required by law.

10. Data Subject Rights

Individuals have rights under the UK GDPR, including:

- Right of access to their personal data
- Right to rectification, erasure, restriction, and objection to processing
- Right to data portability
- Rights related to automated decision-making

The Council will ensure these rights are respected and requests handled promptly.

11. Training and Awareness

- Regular updates will be provided to reflect changes in legislation or best practice.

12. Review

This policy will be reviewed at least every two years or whenever there is a significant change in legislation or council procedures.

Adopted by North Marston Parish Council on: September 2025

Last Review Date: May 2026
Next Review Date: May 2029