



Merriott Parish Council Policy Pack

IT, Data Protection (GDPR), Risk Management & Data Retention

Version: 1.0

Adopted on:

Review Date:

1. Introduction

This Policy Pack sets out how Merriott Parish Council (The Council) manages:

- Information Technology (IT) systems and security
- Personal data in compliance with UK GDPR and the Data Protection Act 2018
- Organisational risk
- Retention and disposal of records

This document supports compliance with:

- The **Accounts and Audit Regulations 2015**
- The **Annual Governance and Accountability Return (AGAR)**, particularly **Assertion 10**
- The **UK General Data Protection Regulation (UK GDPR)**

2. Governance & Responsibilities

2.1 Roles

Full Council

- Approves all policies
- Oversees compliance and governance

Clerk / Responsible Financial Officer (RFO)

- Day-to-day responsibility for:

- Data protection compliance
- IT security
- Records management
- Risk monitoring

Councillors

- Must comply with all policies
 - Use council systems securely
 - Report risks or breaches promptly
-

3. IT & Information Security Policy

3.1 Purpose

To ensure council systems and data are secure, reliable, and protected against loss, misuse, or cyber threats.

3.2 Acceptable Use

- Council IT equipment and email must be used for official business only
- Personal use must be minimal and not compromise security

3.3 Password & Access Controls

- Strong passwords must be used (minimum 12 characters recommended)
- Passwords must not be shared
- Multi-factor authentication (MFA) should be enabled where available

3.4 Data Storage

- Council data must only be stored on:
 - Approved council devices, or
 - Secure cloud services approved by the council
- Personal devices must not store council data unless authorised

3.5 Email Security

- Official communications must use council email accounts
- Suspicious emails must not be opened and should be reported

3.6 Backups

- Data must be backed up regularly (at least weekly)
- Backups must be stored securely and tested periodically

3.7 Cyber Security

- Anti-virus software must be installed and updated
- Systems must be kept up to date with security patches
- The Council will follow guidance from the National Cyber Security Centre (NCSC)
<https://www.ncsc.gov.uk/section/advice-guidance/public-sector>

3.8 Incident Management

- Any IT security incident must be reported immediately to the Clerk
 - Serious incidents must be escalated to the council
-

4. Data Protection (UK GDPR) Policy

4.1 Principles

The council complies with the UK GDPR principles:

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

4.2 Lawful Basis

The council processes personal data under lawful bases including:

- Legal obligation
- Public task
- Consent (where applicable)

4.3 Personal Data Handling

- Only necessary data will be collected

- Data must be accurate and kept up to date
- Data must be stored securely

4.4 Data Subject Rights

Individuals have rights including:

- Access (Subject Access Requests)
- Rectification
- Erasure (where applicable)
- Restriction of processing

Requests must be responded to within **one month**.

4.5 Data Breaches

A breach includes loss, disclosure, or unauthorised access to personal data.

- All breaches must be recorded
- Serious breaches must be reported to the ICO within **72 hours**
- Affected individuals must be informed where necessary

4.6 Privacy Notices

The council will publish clear privacy notices explaining:

- What data is collected
 - Why it is collected
 - How it is used
-

5. Risk Management Policy

5.1 Purpose

To identify, assess, and manage risks that could impact the council's operations, finances, or reputation.

5.2 Risk Register

The council will maintain a **Risk Register** that includes:

- Risk description
- Likelihood and impact

- Mitigation measures
- Responsible person

5.3 Key Risk Areas

Typical risks include:

- Financial mismanagement
- Loss of data
- Cyber security threats
- Legal non-compliance
- Reputational damage

5.4 Risk Review

- Risks must be reviewed at least annually
- High risks must be reviewed more frequently

5.5 Internal Controls

Controls include:

- Financial regulations
- Regular reconciliations
- Audit processes

6. Data Retention & Records Management Policy

6.1 Purpose

To ensure records are retained only as long as necessary and disposed of securely.

6.2 Retention Principles

- Data must not be kept longer than necessary
- Legal and audit requirements must be met
- Disposal must be secure

6.3 Retention Schedule (Summary)

Record Type	Retention Period
Minutes & agendas	Permanently
Financial records	6 years
Contracts	6 years after expiry
Personnel records	6 years after employment ends
Complaints	3–6 years depending on severity
Emails	As required, then deleted

6.4 Disposal

- Paper records: shredded
- Digital records: securely deleted

7. Internal Audit & Assertion 10 Compliance

To meet **AGAR Assertion 10**, the council ensures:

- A **competent and independent internal auditor** is appointed
- Internal audit reviews:
 - Risk management
 - Internal controls
 - Financial systems
 - Governance arrangements
- Findings are:
 - Reported to full council
 - Acted upon promptly

7.1 Evidence of Compliance

The council will maintain:

- Risk Register
- Internal audit reports
- Policy review records

- Minutes showing approval and monitoring
-

8. Training & Awareness

- Councillors and staff will receive appropriate training on:
 - Data protection
 - Cyber security
 - Governance responsibilities
-

9. Monitoring & Review

- This Policy Pack will be reviewed **annually**
 - Updates will reflect:
 - Legislative changes
 - Audit recommendations
 - Emerging risks
-

10. Approval

This Policy Pack was approved by:

Merriott Parish Council

Signed: _____

Name: _____

Position: Chair

Date: _____
