Lytham Town Council
Data Protection and IT Policy

(Adopted: 29/10/2025, Review due: 29/10/2027)

1. Introduction

The purpose of this policy is to ensure that Lytham Town Council (the Council) processes and manages personal data and information assets lawfully, securely, and transparently, in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and guidance from the Information Commissioner's Office (ICO). It also establishes IT governance controls to ensure confidentiality, integrity, and availability of data.

2. Scope

This policy applies to all information handled by the Council, including personal data, financial and operational records, and all IT systems used by councillors, staff, contractors, and volunteers. It also applies to all equipment, email systems, mobile devices, and cloud services used for Council business. This scope includes Council owned and personally owned devices.

3. Legal Framework and Principles

The Council is a Data Controller under the UK GDPR and Data Protection Act 2018. It adheres to the following principles when processing personal data:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

4. Roles and Responsibilities

- **Full Council:** Overall accountability for compliance, approves this policy, and reviews reports annually.
- **Clerk (Responsible Officer):** Operational responsibility for data protection compliance and IT security.
  NB: The Clerk is the Responsible Financial Officer and in addition undertakes the role of the Data Protection Officer for the Council.
- **Data Protection Officer (DPO):** Provides independent advice, monitors compliance, and acts as the contact point with the ICO.
- **Responsible Finance Officer (RFO):** Ensures financial data and AGAR evidence are securely retained.
- **All councillors, staff, and volunteers:** Must handle data responsibly, complete annual training, and report any breaches immediately.

5. Data Processing and Records Management

The Council maintains a Data Inventory documenting each processing activity, lawful basis, purpose, and retention period. Records are retained in line with the Council's retention schedule and the Joint Practitioners' Advisory Group (JPAG) / Annual Governance and Accountability Return (AGAR) requirements.
Minutes and key governance records are permanent; financial and payroll records are retained for at least six years.

6. Information Security and IT Controls

The Council will maintain appropriate technical and organisational measures including:

- Role-based access controls and secure passwords – including for website management
- Use of council owned and managed email accounts for official business which are structured in accordance with existing requirements and which make use of .gov.uk domain security
- Multi-factor authentication for administrative accounts
- Secure storage and effective policy governing the use of Audio Recording of public meetings for the purpose of accurately completing minutes.
- Multi-signatory access controls for online banking accounts
- Use of Scribe Accounts software for financial management has existing and tested security regimes. Access can be opened up for Read / Write and Read Only – thereby enabling remote access in a Read Only format for Councillors and Independent Auditors.
- Encryption of portable devices and backups
- Regular system updates and patch management
- Secure disposal of paper and electronic records
- Backup and disaster recovery testing
- Anti-virus and endpoint protection software

7. Website Accessibility

The website run by the Council https://lythamtowncouncil.gov.uk complies with web accessibility standards and an Accessibility Statement is included within the website itself at https://www.lythamtowncouncil.gov.uk/accessibility-

statement/#:~:text=For%20example%2C%20that%20means%20you,of%20JAWS%2C%20NVDA%20and%20VoiceOver)

8. Subject Access Requests (SAR)

Individuals have the right to access personal data held by the Council. Requests should be submitted in writing using the SAR form at Appendix B. The Clerk or DPO will respond within one calendar month. All requests are logged, and identification checks are performed before disclosure.

NB: At the time of writing, it is the Council's intention to create this as a Web based form embedded within the Website to ensure effective accessibility.

9. Data Breach Management

All actual or suspected data breaches must be reported immediately to the Clerk. Breaches will be assessed using the checklist in Appendix C. Where there is a risk to individuals' rights and freedoms, the ICO will be notified within 72 hours, and affected individuals will be informed where required.

10. Data Protection Impact Assessments (DPIAs)

DPIAs are required for any new or significantly changed processing that may result in high risk to individuals, such as CCTV, new IT systems, or sharing arrangements. The DPIA template at Appendix D will be used to document assessment and mitigation.

11. Training and Awareness

All councillors, staff, and volunteers handling personal data must complete annual data protection training. Training records will be maintained by the Clerk. The Council will also provide refresher briefings following any major policy or legal change.

12. Monitoring and Review

This policy will be reviewed every two years or sooner if required by changes in legislation, guidance, or council practice. The Clerk and DPO are responsible for proposing updates for Council approval.

Version Control

Version	Date	Description of Change	Author
V1	29/10/2025	Policy approved and adopted	Luke Russell C/RFO

Appendices

Appendix A – Data Inventory Overview

The Council maintains a detailed Data Inventory (register) of all personal data processing activities, including purpose, lawful basis, data subjects, categories of data, retention periods, and processors. A summary of key datasets is provided in the Excel file (LTC_Data_Inventory.xlsx) stored in the Clerk's File directory

Appendix B – Subject Access Request (SAR) Form

Use this form to request access to your personal data held by Lytham Town Council.
Name:
Address:
Email:
Description of Information Requested:
Proof of Identity Provided:
Date Received:
Response Due Date:

Appendix C – Data Breach Log & Checklist

All data breaches or near misses must be recorded. The checklist includes:
1. Description of incident
2. Type and volume of data affected
3. Containment actions
4. Assessment of risk to individuals
5. Notification required (ICO / data subjects)
6. Lessons learned and preventive actions

Each entry in the Breach Log must be numbered, dated, and signed by the Clerk or DPO.

Appendix D – Data Protection Impact Assessment (DPIA) Template

Project / Processing Activity:
Purpose of Processing:
Categories of Data and Subjects:
Lawful Basis:
Risk Assessment (likelihood and severity):
Mitigation Measures:
Consultation (if applicable):
DPO Comments:
Date Completed:
Review Date: