Ramsgate Town Council

IT POLICY

Adopted	**28 January 2026**
Due to review	**Every three years.**

Executive Summary

The Ramsgate Town Council IT Policy ensures that the Council IT systems are used securely, legally, and responsibly. This policy, working in conjunction with others set out by the Council, sets out clear responsibilities, acceptable use standards, and procedures for managing IT-related risks.

Who's Responsible

- Full Council approves policy.
- Finance and General Purposes Committee oversees IT, risks, and compliance.
- Town Clerk (Data Controller) acts as data protection lead.
- Responsible Financial Officer (RFO) secures financial systems and backups.
- Councillors, Staff, Volunteers follow the policy, complete training and report incidents.
- External IT Providers handle the day-to-day IT and must comply with Council policies and contracts.

Key Rules

✅ Use Council email for official business.
✅ Store data only on authorised systems.
✅ Keep devices secure with passwords, Two-factor authentication (2FA) and updates.
✅ Report lost devices, suspicious emails, or breaches immediately.
❌ Don't share passwords or forward Council information to personal accounts.
❌ Don't install unapproved software or hardware.
❌ Don't use Council IT for personal financial gain or inappropriate activity.

Devices

- Council-issued devices remain Council property.
- Devices must be returned at the end of service.
- Equipment replaced on a set cycle. (There will be a rolling programme of renewals).

Data & Compliance

- Follow GDPR, Data Protection & Retention Policy, Privacy Policy.
- Respect Accessibility, Copyright, Communications, and CCTV Policies.
- Backups and encryption protect sensitive data.

Training

- Induction training for all new councillors and staff.
- Annual refresher training on data protection, cybersecurity, and acceptable use.

Incident Reporting (Quick Steps)

1. Report immediately to the Town Clerk.
2. The Town Clerk investigates and logs the issue.
3. If data is at risk, the Information Commissioners Officer (ICO) will be notified within 72 hours of becoming aware of the breach, where required.
4. The Council will review and ensure corrective action is taken.

Review Cycle

This policy is to be reviewed every three years or after significant changes or incidents occur.

Contents

1. Purpose and Scope

This IT Policy sets out the standards for the secure, efficient, and responsible use of Ramsgate Town Council's (the Council) IT resources. It applies to all councillors, employees, contractors, and third parties who use Council systems, devices, or data.

The objectives are to:

- Protect the confidentiality, integrity, and availability of Council information.
- Ensure compliance with legislation including General Data Protection Regulation (GDPR), Freedom of Information (FOI), and Copyright Law.
- Support digital transparency, accessibility, and effective communication with residents.

2. Governance and Responsibilities

Clear roles and responsibilities ensure effective IT governance within the Council.

Full Council

- Approves and adopts this policy and any major amendments.
- Ensures resources are available to support IT security and renewal.

Finance and General Purposes Committee

- Oversees implementation of this policy.
- Reviews IT performance, risks, and compliance.
- Recommends updates to Full Council.

Town Clerk (Proper Officer)

- Acts as the Data Controller under GDPR.
- Responsible for day-to-day IT compliance and security.
- Authorises user access levels.
- Coordinates with external IT providers (where contracted).

Responsible Financial Officer (RFO)

- Oversees IT systems related to financial management.
- Ensures secure data storage, backups, and access to financial systems.

Councillors, Staff, and Volunteers

- Must follow this policy at all times.
- Complete mandatory IT and Data Protection training.
- Report any IT incidents, suspected breaches, or equipment loss immediately to the Town Clerk.

External IT Providers

- Provide technical support, maintenance, or security services under contract.
- Must comply with this policy and relevant data protection legislation.
- Contracts with external IT providers must include confidentiality, data protection, and security obligations.

3. **Compliance with Legal and Council Policies**

All IT use must comply with legislation and Ramsgate Town Council policies, as listed below:

- **Accessibility Statement**
  This statement requires all digital communications to be inclusive and accessible.

- **Artificial Intelligence (AI) Policy**
  This policy governs the acceptable and responsible use of AI tools in support of Council business.

- **CCTV Policy**
  This policy governs the monitoring and use of recorded footage.

- **Communications Policy, Press and Media Communications Procedure, Emergency Communications Procedures**
  These policies govern the use of email, websites and social media.

- **Copyright and Usage Policy**
  This policy ensures lawful use of digital materials.

- **Data Protection and Retention Policy**
  This policy governs how personal and sensitive data is handled, stored, and disposed of.

- **Personal Portable Appliance (PAT) Policy**
  This policy covers safe use and testing of electrical devices.

- **Privacy Policy**
  This policy outlines how data is collected and processed.

4. **Acceptable Use of IT Resources**

Council IT resources are primarily for official business. Limited personal use may be permitted in exceptional circumstances, subject to approval by the Town Clerk, and provided it does not compromise security, performance, or the reputation of the Council.

Permitted Use

- Using Council email accounts for official correspondence, i.e. ramsgatetowncouncil.gov.uk.
- Storing Council data on authorised systems only (e.g., Onedrive / SharePoint - the approved cloud storage).
- Conducting Council meetings and business via authorised platforms.
- The use of Artificial Intelligence (AI) tools for Council business is permitted only in accordance with the Councils Artificial Intelligence (AI) Policy.

Prohibited Use

- Accessing, storing, or sharing inappropriate or offensive content.

- Forwarding Council information to personal email accounts.
- Installing unauthorised software or hardware.
- Circumventing security (e.g., password sharing, disabling antivirus).
- Using Council IT for personal financial gain, political campaigning (outside official duties), or commercial activity. (Council IT equipment should only be used for Council business).
- AI tools must not be used in a way that breaches the Artificial Intelligence (AI) Policy, Data Protection and Retention Policy, or Privacy Policy.
- Users must not input personal, sensitive, confidential, or commercially sensitive Council data into AI systems unless explicitly permitted by the AI Policy.
- AI tools must not be used to make automated decisions or recommendations without appropriate human oversight.

Devices and Equipment

- Councillors and staff will be issued Council devices (e.g., laptops, tablets or phones).
- Devices must be returned when leaving office or employment.
- Equipment will be replaced on a planned renewal cycle (There will be a rolling programme of renewals).
- All equipment must comply with the PAT Policy.

5. Training and Awareness

- New councillors and staff will receive IT and Data Protection induction training.
- Annual refresher training will be provided covering cybersecurity, GDPR, and acceptable use.
- Additional training will be delivered when new systems are adopted.

6. Incident Reporting and Response

All IT incidents must be reported immediately to the Town Clerk. Examples include:

- Lost or stolen devices.
- Phishing emails or suspected malware.
- Unauthorised access attempts.
- Data breaches or accidental disclosure of information.

Procedure:

1. User reports incident to the Town Clerk immediately.
2. The Town Clerk investigates and logs the incident.
3. If personal data is affected, the Town Clerk will assess the risk and notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where required.
4. The Council reviews incidents and ensures corrective action is taken.

7. Review

This policy will be reviewed every three years, or sooner if: required by law, technology changes, or after a significant IT incident.