Redgrave Parish Council

INFORMATION TECHNOLOGY POLICY

Policy Statement

This Information technology (IT Policy) sets out how Redgrave Parish Council (the Council) manages IT, digital records and electronic communications. It supports compliance with Assertion 10 of the Annual Governance and Accountability Return (AGAR), confirming that the Council has appropriate arrangements in place to safeguard data, manage risks, and ensure the secure and reliable use of IT systems.

The policy is based on the National Association of Local Councils (NALC) template and has been adapted to reflect the size, capacity and operating arrangements of the Council.

Scope

This policy applies to:

- Councillors
- The Clerk / Responsible Financial Officer (RFO)
- Employees, contractors and volunteers acting on behalf of the Council

It covers all IT systems and devices used to conduct Council business, including:

- The parish-supplied computer issued to the Clerk / RFO
- Personal computers, laptops, tablets and mobile phones used by councillors for Council business
- Email accounts
- Cloud-based services and storage
- The Council website and social media
- Digital records and backups

Roles and Responsibilities

The Council

The Council is responsible for:

- Approving and reviewing this IT Policy
- Ensuring adequate resources are available for secure IT systems
- Receiving assurance that IT risks are identified and managed

Clerk / Responsible Financial Officer

The Clerk/RFO is responsible for:

- Day-to-day management of Council-owned IT systems

- Ensuring data is stored securely and backed up
- Maintaining passwords and access controls
- Reporting any IT security incidents or data breaches to the Council
- Ensuring compliance with data protection legislation

Councillors and Users

All users must:
- Use Council-owned IT systems responsibly and only for Council business
- Protect passwords and not share login details
- Report suspected security incidents immediately

Comply with this policy and related policies

IT Systems and Equipment

- Council-owned equipment must be used where possible.
- Where personal devices are used, they must be adequately protected with passwords and up-to-date security software.
- Software must be legally licensed and kept up to date.
- Devices must be locked when unattended.

Passwords and Access Control

- Strong passwords must be used for all Council-owned systems.
- Passwords must not be shared.
- Two-factor authentication should be used where available.
- Access to Council-owned systems will be restricted to those who need it to perform their role.

Data Management and Storage

- Council data will be stored securely, either on encrypted devices or reputable cloud services.
- Personal data will be processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- Only the minimum necessary data will be collected and retained.
- Data retention will follow the Council's Records Management and Retention Policy.

Backups and Business Continuity

- Regular backups of Council data will be taken.
- Backups will be stored securely and separately from live systems.
- Backup arrangements will be tested periodically.

These measures support business continuity and reduce the risk of data loss, in line with Assertion 10 requirements.

Email and Electronic Communications

- Council business should be conducted using Council email accounts wherever possible.
- Emails may be subject to Freedom of Information requests and must be written accordingly.
- Suspicious emails or attachments must not be opened and should be reported to the Clerk.

Website and Social Media

- The Council website will be maintained to ensure accuracy, security and accessibility.
- Content must be lawful, respectful and appropriate.
- Social media accounts, where used, will be managed in accordance with the Council's Communications Policy.

Cyber Security and Risk Management

The Council recognises cyber security as a key governance risk and will:

- Keep systems and software updated
- Use antivirus and firewall protection
- Ensure regular backups
- Review IT risks as part of the Council's risk management arrangements

These controls provide assurance that IT risks are properly managed, supporting compliance with Assertion 10.

Data Breaches and Incidents

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

Monitoring, Review and Governance

- Compliance with this policy will be monitored by the Clerk.
- The policy will be reviewed at least annually, or sooner if there are significant changes to legislation, technology, Council operations, SAPPP guidance, or best practice.

Compliance with this policy will be confirmed as part of the Annual Governance and Accountability Return (AGAR) review process.

Related Policies

This policy should be read in conjunction with:

- Data Protection Policy
- Records Management and Retention Policy
- Risk Management Policy
- Freedom of Information Policy