READ
PARISH COUNCIL

Read Parish Council IT Policy

Introduction

Read Parish Council recognises the importance of secure and effective Information Technology (IT). This IT Policy provides a clear and simple guide that outlines how technology is used, how data is protected, and how council business is conducted securely online.

Scope

This policy applies to all councillors, employees, contractors, and volunteers who use IT systems to carry out the council business of Read Parish Council, whether on council-owned or personal devices.

The IT policy covers all IT resources used by the Parish Council, including, Computers, laptops, tablets, smartphones, networks, software and data.

Acceptable use of IT Resources

Read Parish Council has a duty to ensure effective and secure use of technology. IT resources and email accounts are to be used for official Council related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy.

The Council require all official communications to use a council owned email address (e.g. clerk@read-pc.gov.uk). The Clerk and all Councillors at Read Parish Council have a Parish Council email address used exclusively for parish council business.

Members of the Parish Council using a Council laptop must not install additional software without permission.

All login details and passwords are to be kept secure.

Data Protection and GDPR

All users must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This includes:

- Keeping personal data secure and confidential.
- Not disclosing information without proper authorisation.
- Using encryption and secure storage where required.

IT Equipment and Licences

Read Parish Council provide the Clerk with a laptop for exclusive use of Parish Council business.

The Office 365 licence (Microsoft Outlook, Word, Excel etc) is licensed to (and paid for) by Read Parish Council.

Website Management

Read Parish Council website is managed by Easy Webs Sites Ltd. The website is compliant with WCAG 2.2AA standards.

The website includes all required documentation. The clerk is responsible for publishing the Agenda, Minutes, AGAR Documents and all relevant Council information.

For security the password for the CMS (content management system) is a combination on lowercase and uppercase letters, numbers and special characters.

Easy Web Sites Ltd installs SSL (Secure Socket Layer) certificates to encrypt all data transmission between the server and users' devices. This ensures that sensitive information such as passwords, credit card numbers, and personal data is protected during transmission.

To comply with the guidelines from National Association of Local Councils (NALC), Read Parish Council have the website hosted under a .gov.uk.

Email Management

Easy Web Sites provide the email services for Read Parish Council. Easy Web Sites Ltd uses IONOS, a major email hosting provider, to host emails. IONOS implements industry-standard security protocols to protect client email data and systems from potential cyber security risks.

All Councillors are provided with a Parish Council .gov.uk email address for exclusive use of Parish Council business.

The emails are provided and supported by Easy Web Sites Ltd who provide the following support services;

1. Creating emails with a secure password. Councillors are not permitted to create or use their own (easy to remember) passwords, for security. Passwords are a combination on lowercase and uppercase letters, numbers and special characters.

2. Changing passwords (if a Councillor was no longer in post)

3. Deleting the email box in the event that a Councillor is no longer in the post through resignation or death

Should a Councillor no longer be in the position then the email box and all the content may at the discretion of the Council be immediately deleted.

Read Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

Reporting security Incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact (Easy Web Sites) for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator (Easy web Sites) immediately.

Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

Policy Adopted	Policy Reviewed	Next Review
February 2026		February 2027