

Minstead Parish Council IT Policy

Adopted on: 6th October 2025
Review Date: 1st October 2027

1. Purpose

This policy outlines how Minstead Parish Council manages and uses its IT resources to support its work, safeguard data, and comply with legal obligations.

The laws relating to this policy are:

- Data Protection Act 2018 and the UK General Data Protection Regulations 2016:
These laws mandate how organisations collect, store, process, and protect personal data of UK residents, requiring fair and transparent data handling, security measures, and data subject rights. The Council holds a separate Data Protection Policy.
- Freedom of Information Act 2000
- Transparency Code for Smaller Authorities
- Computer Misuse Act 1990: This act addresses unauthorised access to computer material, modification of data, and related offenses, setting penalties for hacking and other cybercrimes.
- Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018

Relevant Council policies:

- Data Protection
- Freedom of Information
- Available Documents and charges (Publication Scheme)
- Retention of Documents timescales

2. Scope

This policy applies to all councillors, employees, and volunteers who access or use Parish Council IT systems, including computers, emails, internet access, mobile devices, and cloud services. It applies to personal information only.

3. Acceptable Use of Council provided equipment

The Council laptop must be password protected and turned off when not in use.
The laptop PIN is known to the Clerk / RFO, the IT administrator and the Chair.

Council IT resources must be used only for Council-related activities.

Personal use should be limited, appropriate, and not interfere with Council duties.

Users must not access, download, or send inappropriate or illegal material.

4. Emails, Mobile phones and Communication

Use only Council email addresses for Council business, and where Councillors use their own laptops for Council business, the Council email account must be password protected.

Where Councillors use their own mobile phones for Council-related email and WhatsApp communication, those phones should be protected from unauthorised access.

Be professional and courteous in all communications. Do not include illegal or discriminatory content.

Agreements with suppliers incurring expenditure must only be entered into using email by the Clerk, or in the Clerk's absence, by the Chair.

Do not share personal information relating to an identifiable individual without proper authority. If in doubt refer to the Council's Data Protection policy.

5. Data Protection and Security

Follow UK GDPR and Data Protection laws, if in doubt refer to the relevant Council policies as listed above.

The Council's Data Protection Officer is the Minstead Parish Council Clerk and Responsible Finance Officer.

Personal data is collected and stored only when lawful and necessary for Council records and transparency requirements. The data collected is believed to be accurate and is stored only as long as necessary in accordance with UK legal requirements and the Council's Retention of Documents timescales.

Electronic files are stored securely on password-protected Cloud storage.

Report data breaches or loss of Council data to the Data Protection Officer immediately.

Passwords are held by the Data Protection Officer. A copy of the passwords is held by the Chair in a sealed envelope. The envelope is to be accessed in the event of the Data Protection Officer's incapacity or inability for whatever reason, to be able to access the passwords.

Passwords are changed when Clerks change, and bank account access is changed when Councillors with access to the Council bank account leave the Council.

6. Accessibility

The Council has an obligation to meet the Web Content Accessibility Guidelines (WCAG) 2.2 AA accessibility standard.

Where this is not possible, the Council has published an Accessibility statement on the front page of the Parish Council web pages, explaining where the Guidelines are not met and informing members of the public how they may access information in accessible formats.

7. Software and Hardware

Only use authorised and licensed software on Council-owned IT equipment.

Do not install personal or unapproved software on Council-owned IT equipment.

Report any damage, loss, or malfunction to the Clerk.

8. Social Media and Websites

Use social media responsibly and in accordance with Council policies when representing the Council.

Only authorised persons may post on official Minstead Parish Council platforms.

Avoid sharing personal opinions as if they are Council positions.

9. Remote Working

Use secure internet connections when working remotely.

Keep paper and digital files as confidential at home or on the move. Paper files must be in closed cupboards at home and kept safe from unauthorised viewing when away from home.

10. Monitoring and Compliance

The council reserves the right to monitor IT usage in line with privacy laws.

Breaches of this policy may result in disciplinary action or referral to relevant authorities.

11. Review

This policy will be reviewed every two years or when there are significant changes in technology or legislation.

Signed:

William Andrews, Chair of the Parish Council:

Diana O'Grady, Clerk to the Parish Council:

Date: 6th October 2025