NETTLEBED PARISH COUNCIL

IT Policy

Reviewed by:	Full Council
Review / Adopted date:	2nd February 2026
Next Review date:	February 2029

NETTLEBED PARISH COUNCIL

IT POLICY

Introduction

This policy explains how councillors, staff, and authorised users should use council IT systems and equipment.

It protects council data, ensures safe and responsible use, and clarifies acceptable and unacceptable behaviour

It applies to council-provided devices and authorised personal devices used for council business.

Purpose of the IT Policy

The policy aims to:

- Protect council data and equipment
- Set expectations for acceptable IT use
- Clarify consequences of misuse
- Support compliance with the UK GDPR and Data Protection Act 2018

Limited personal use of council equipment is permitted (e.g checking personal email during breaks) but must not interfere with council work.

Monitoring of IT use

The council may monitor IT systems to:

- Maintain security and prevent misuse
- Investigate faults or breaches
- Comply with legal obligations

Monitoring will be proportionate, respect privacy laws, and apply to council devices and authorised personal devices used for council purposes.

Information may be shared internally or with professional advisers if necessary.

Scope of this policy

Applies to all councillors, staff, and authorised users, whether working at home, council premises, or elsewhere.

Covers council equipment and authorised personal devices used for council business.

NETTLEBED PARISH COUNCIL

IT POLICY

Computer Use

1. Hardware

1.1. Council devices are provided for council business - limited personal use is allowed during breaks or outside working hours.
1.2. Lock devices when unattended.
1.3. Treat all equipment carefully and keep it clean.
1.4. Equipment must not be dismantled or software installed without authorisation.
1.5. Personal storage devices (USBs etc) require approval before use.

Equipment

2. Portable equipment

2.1. Includes laptops, tablets, mobile phones, and other portable devices.
2.2. Lock devices when unattended.
2.3. Store devices securely when not in use; do not leave unattended in public or vehicles.
2.4. Devices must be password-protected or encrypted - enable auto-wipe if available.
2.5. Report any loss, theft, or damage immediately.

3. Use of own devices

6.2.1 Councillors and staff may use personal devices to access council emails or documents provided:

- Emails are sent from council accounts only
- Work and personal data are kept separate
- Devices are secure with strong passwords or PINs
- Lost or compromised devices are reported immediately

6.2.2 The Clerk may use a personal landline for council calls if necessary (e.g. freephone numbers likely to involve long holds).

6.2.3 Councillors may store council documents on personal devices but must maintain confidentiality and comply with security rules.

8 Password and account security

8.1 Use strong passwords (e.g., three random words) and change them if compromised.

8.2 Multi-Factor Authentication (MFA) to be enabled where possible.

8.3 Passwords are personal and must not be shared.

8.4 Administrative passwords must be securely stored and only accessed in emergencies.

9 Monitoring

9.1 The council may monitor:

- Emails, internet use, and files on council devices
- Activity on authorised personal devices used for council work

9.2 Monitoring is for security, compliance, and fault investigation.
9.3 Information may be shared internally or with professional advisers.
9.4 Monitoring is proportionate and respects privacy laws.

10 Remote working

10.1 Devices used remotely must remain secure.

10.2 Do not leave devices or printed documents unattended.

10.3 Use secure WiFi, encryption, and screen privacy filters when handling council data remotely.

10.4 Remote wipe functions should be enabled where possible.

10.5 Limit the use of paid-for WiFi/dongles to essential council purposes only.

11 Email

11.1 Council emails are primarily for council business - minimal personal use is allowed during breaks.

11.2 Emails must be professional and sent from council accounts only.

11.3 Sensitive attachments should be password-protected.

11.4 Council numbers should be used for work-related calls where possible.

12 Use of a Council provided internet service

12.1 Comply with copyright, data protection, and other relevant laws.

12.2 Accessing inappropriate websites or services is strictly prohibited.

12.3 Verify accuracy of online information before using it for council purposes.

13 Use of social media

13.1 Be careful when posting online, even from personal accounts.

13.2 Do not share confidential or sensitive council information.

13.3 Make it clear that personal opinions are your own.

13.4 Avoid posts that could harm the council's reputation.

13.5 Council contacts and data remain council property and must not be used for personal social media without authorisation.

14 Misuse

14.1 Misuse of IT systems or council data may result in disciplinary action.

14.2 Examples include:

- Unauthorised access or sharing of council information
- Using council systems for illegal or inappropriate activity

15 Guidance

15.1 If unsure about IT use, consult the Clerk or council IT provider.

15.2 Protect council data on personal devices.

15.3 On leaving the council, remove all council data from personal devices.