Nempnett Thrubwell Parish Council

Password & Device Security Policy

Adopted June 2026 (Next Review June 2027)

1. Purpose

This policy sets out the council's approach to passwords and basic device security. Its purpose is to protect council information, reduce the risk of unauthorised access, and demonstrate good governance and internal control in line with data protection requirements and Assertion 10.

This policy applies to councillors, officers, contractors and anyone who accesses council information or systems.

2. Scope

This policy covers:

- Council email accounts and shared mailboxes
- Cloud storage and file-sharing systems
- Council-owned devices
- Personal devices used for council business

3. Password standards

Passwords must:

- Be made up of **three random words separated by dots** (e.g. river.clock.apple)
- Be unique to council systems and **not reused** elsewhere
- Not include the name of the council, staff names, councillor names, locations, or anything easily guessed

Passwords must not:

- Be shared with others

- Be written down and stored insecurely
- Be reused after a password reset or role change

4. Password changes

Passwords must be changed:

- Periodically, as part of routine good practice
- **Immediately** when a councillor or member of staff leaves the council
- When a role changes and access is no longer required
- If there is any concern that a password may have been compromised

Shared or generic passwords (where unavoidable) must be changed whenever access arrangements change.

5. Device security

All devices used for council business must:

- Be protected by a PIN, password or biometric lock
- Automatically lock when not in use
- Be kept up to date with system and security updates where possible

This applies to both council-owned devices and personal devices used for council work.

6. Councillor responsibilities

Councillors are responsible for ensuring that:

- Their council email account is protected by a strong password
- Any device used for council business is appropriately locked
- Council information is not accessed or viewed by unauthorised individuals

7. Support and compliance

No one is expected to be an IT specialist. Support is available where required, and reasonable steps will be taken to help users comply with this policy.

Failure to follow this policy may increase risk to the council and will be addressed proportionately and supportively.

8. Review

This policy will be reviewed periodically and updated as required to reflect changes in technology, working practices, or regulatory guidance.