

Deene & Deenethorpe Parish Council

Information Technology Policy

- **1. Introduction**

Deene & Deenethorpe Parish Council uses information technology to support its statutory functions and day-to-day operations. Each council's IT setup differs, and this policy is tailored to the needs of a small parish council. It sets out how councillors, staff, and authorised users must use council IT systems safely, responsibly, and in compliance with legal requirements.

Councils using external IT providers must ensure this policy reflects current practices and contractual arrangements.

- **2. Purpose of the IT Policy**

This policy aims to:

- Set expectations for appropriate use of council IT equipment and systems
- Raise awareness of risks associated with IT use
- Safeguard council data and digital assets
- Clarify acceptable and unacceptable use
- Support compliance with UK GDPR, the Data Protection Act 2018, and NCSC guidance
- Outline consequences of policy breaches

Limited personal use of council IT equipment may be permitted where authorised and where it does not interfere with council business.

- **3. Monitoring of IT Use**

The council may monitor use of its IT systems where there is a legitimate reason to do so. Monitoring must be proportionate and comply with data protection and privacy laws. Users will be informed that monitoring may take place.

Monitoring may include internet usage logs, email activity, access logs, and security scans. Monitoring will follow the Investigatory Powers (Interception by Councils etc.) Regulations 2018.

- **4. Scope of the Policy**

This policy applies to:

- Councillors
- The Clerk and any employees
- Contractors or volunteers with authorised access
- Any person using council IT systems or council email accounts

It applies whether users are working in the office, at home, or remotely.

- **5. Computer Use**

5.1 Hardware

- Council IT equipment is provided primarily for council business. Limited personal use may be permitted at the Clerk's discretion.
- Users must lock their screens when leaving their workstation.
- Equipment must be treated with care and kept clean.
- Food and drink should not be placed near devices.
- All council equipment will be asset-tagged and logged.
- Users must not dismantle equipment or install software without approval.
- Personal USBs or storage devices may not be used without prior authorisation.
- Faults or damage must be reported to the Clerk or IT provider.

- **6. Portable Equipment**

Portable equipment includes laptops, tablets, mobile phones, and similar devices.

6.1 Security & Storage

- Devices must be stored securely and never left unattended in vehicles or public places.
- All portable devices must use encryption and PIN/password protection.
- Multi-Factor Authentication (MFA) should be used wherever possible.
- Remote wipe capability must remain enabled where available.

6.2 Loss or Theft

Loss or theft must be reported immediately. Users must retain IMEI/SIM details for mobile devices.

6.3 Cameras & Recording

- Photographs or recordings on council premises require written permission from the Clerk.
- No private meeting may be recorded without consent.

- **7. Use of Personal Devices (BYOD)**

Personal devices may be used for council work only with prior approval.

Users must:

- Use strong passwords (three-random-words method)
- Keep devices updated and patched
- Use council email accounts for council business
- Keep council data separate from personal data
- Avoid saving council data to personal cloud accounts
- Ensure family members cannot access council information
- Report loss, theft, or compromise immediately

Sensitive council data must not be stored on personal devices.

- **8. Health & Safety**
- Workstations will be set up appropriately for users.
- DSE assessments and eye tests will be offered in line with council policy.
- Hazards or unusual noises from equipment must be reported immediately.

- **9. Password & Authentication Policy**

The council follows NCSC guidance on strong passwords using the three-random-words method.

9.1 Requirements

- Passwords must not be shared.
- Administrative credentials will be securely stored, with emergency access held by the Chair.
- Passwords must be stored in an approved encrypted password manager.
- Passwords must be changed immediately if compromise is suspected.

- MFA must be used where available.

- **10. Monitoring**

The council reserves the right to monitor IT usage to ensure compliance with this policy, maintain system security, and investigate faults or misconduct. Monitoring will be proportionate and compliant with UK GDPR.

Information obtained through monitoring may be shared internally or with external advisers where necessary. Data will be retained only as long as required.

- **11. Remote Working**

Users working remotely must:

- Avoid saving passwords on shared or public devices
- Position screens to prevent overlooking
- Securely store and dispose of printed documents
- Avoid leaving council data in vehicles
- Use privacy filters when handling sensitive data
- Use secure Wi-Fi and encrypted channels (VPN/HTTPS)

- **12. Email Use**

- Council email accounts are for council business.
- Personal use is permitted only where authorised and must not interfere with council work.
- Users should choose the most effective communication method (email, phone, or face-to-face).
- Emails must not contain offensive, discriminatory, or inappropriate content.

- **13. Use of the Internet**

13.1 Copyright

Users must comply with copyright law. Copying online content without permission is prohibited.

13.2 Trademarks & Links

- New domain names or trademarks may only be registered with council approval.
- External links from council webpages require Clerk approval.

13.3 Data Protection

Users must comply with the council's Data Protection Policy when handling personal data.

• 14. Use of Social Media

14.1 Purpose

Social media is used to communicate with residents, share information, and support transparency. This section governs official and personal use.

14.2 Council-Managed Accounts

- The Clerk is the primary administrator.
- Content must be factual, respectful, non-political, and GDPR-compliant.
- The council will not publish personal data without consent or content that may bring the council into disrepute.

14.3 Engagement & Moderation

- The Clerk responds to queries where appropriate.
- The council will not engage in arguments online.
- Offensive or inappropriate comments may be removed or hidden.
- Repeat offenders may be blocked.

14.4 Councillors' Personal Use

Councillors must:

- Follow the Code of Conduct
- Avoid posting confidential information
- Not claim to speak for the council unless authorised
- Distinguish personal views clearly

14.5 Staff Use

Staff must not post on behalf of the council unless authorised and should avoid discussing council business online.

14.6 Data Protection

Personal data must not be shared on social media without consent. Sensitive matters must be handled through formal processes.

14.7 Security

Passwords must follow council policy. MFA should be used. Lost or compromised credentials must be reported immediately.

14.8 Breaches

Breaches may result in withdrawal of access, Code of Conduct investigation, disciplinary action, or referral to external authorities.

- **15. Breaches of Policy**

Breaches of this IT Policy may result in:

- Withdrawal of IT access
- Investigation under the Member Code of Conduct
- Disciplinary action for staff
- Termination of contractor agreements
- Referral to external authorities where required

- **16. Review**

This policy will be reviewed annually or sooner if required due to changes in legislation, technology, or council practice.

Reviewed 28/09/2026

Next Review 09/2027