DOWNTON PARISH COUNCIL

IT RESOURCES & INFORMATION SECURITY POLICY

The purpose of this Policy is to set-out guidelines and responsibilities for the: -

1. appropriate use of the Council's IT resources and emails
2. protection of the Council's information assets from threats (whether internal or external, deliberate or accidental)
3. confidentiality, integrity, and availability of Council data in line with legal and regulatory requirements e.g. General Data Protection Act (GDPR), UK Data Protection Act 2018 (DPA).

Approved and adopted by a Meeting of the Council held on 14 July 2025.

Signed:	Melanie Camilleri (Proper Officer and Responsible Financial Officer)
Signed:	Cllr Jane Brentor (Chair)
Date:	14 July 2025

1. Introduction

Downton Parish Council (the Council) is committed to the: -

1. appropriate use of the Council's IT resources and emails
2. protection of the Council's information assets from threats (whether internal or external, deliberate or accidental)
3. confidentiality, integrity, and availability of Council data in line with legal and regulatory requirements e.g. GDPR and DPA.

These matters are vital for any Council meeting its statutory obligations and retaining the public's trust.

The Practitioners' Guide 2025 stipulates that all smaller authorities must have an IT Policy which explains how Councillors and Officers should conduct authority business in a secure and legal way when using IT equipment and software (both Council owned and personal equipment). Section 1 - Annual Governance Statement of the Annual Governance and Accountability Returns for 2025/26 onwards contains a new Assertion 10: 'Digital and data compliance'. To warrant a positive response to this assertion, the Council needs to have taken actions on points 1.45-1.54 of the Guide. 1.54 states that all smaller authorities must have an IT Policy.

2. Scope

This Policy applies to Councillors and Officers of the Council.

3. Acceptable use of IT resources and email accounts

Officers

Council owned, role specific, .gov.uk email accounts will be provided to Officers for the purposes of carrying out Council business, operations, and communications. Personal use of these .gov.uk email accounts is strictly prohibited.

Council owned computers and devices will be provided to its Officers for the purposes of carrying out Council business, operations, and communications. These computers and devices will be itemised on the Council's Asset Register. Restrictions of their use: -

- Installation of unauthorised software is strictly prohibited due to security concerns
- Limited personal use is permitted provided it does not: -
  - interfere with work responsibilities
  - involve accessing inappropriate or high-risk websites, illegal activity, political campaigning, or personal business
  - violate any part of this Policy

Officers may, with the Council's consent, use a personal computer and device for the purposes of carrying out Council business, operations, and communications. Use of a personal computer and device is subject to the conditions set-out in the 'Personal Computers and Devices' section of this Policy.

Councillors

Council owned, Councillor name specific, .gov.uk email accounts will be provided to Councillors for the purposes of carrying out Council business, operations, and communications. Personal use of these .gov.uk email accounts is strictly prohibited.

The Council does not supply computers and devices to its Councillors. Councillors must therefore use personal computers and devices for the purposes of carrying out Council business, operations, and communications. Use of a personal computer and device is subject to the conditions set-out in the 'Personal Computers and Devices' section of this Policy.

Personal Computers and Devices

All Councillors (and Officers with the Council's consent) may use their personal computer and device for the purposes of carrying out Council business, operations, and communications subject to compliance with Sections 4 and 5 of this Policy i.e.: -

- Council systems e.g. .gov.uk email account, Dropbox must be accessed via secure methods i.e. web based, password protected.
- personal computers and devices must be installed with reputable anti-virus, anti-spyware, and firewall software, as agreed by the Council
- access to Council data is strictly prohibited from any family member or unauthorised person who has access to and use of the personal computer and device
- security incidents such as a suspected loss, breach, or theft of a personal computer or device must be reported to the Council's Clerk and Chair within 24 hours of the incident occurring
- upon leaving the Council, immediately delete all Council data and access to Council systems from personal computers and devices, and confirm in writing to the Council's Clerk or Chair that this has been done

4. Information Security

Information Security (InfoSec) is the protection of important information against unauthorised access, disclosure, use, alteration, or disruption. It ensures the confidentiality, integrity, and availability of Council data in compliance with legal and regulatory requirements.

a) IT Security

IT Security is concerned with protecting physical and digital IT assets but does not include protection for the storage of paper files.

To protect the Council's physical and digital IT assets, Councillors and Officers are responsible for: -

- Creating strong, secure passwords to access those assets e.g.: -
  - Password creation options, if available: -
    - a combination of words, numbers, symbols, both upper and lower case letters
    - PIN nos
    - biometric authentication
    - two-factor authentication
  - Password security: -
    - treat all passwords as sensitive, confidential information
    - do not use work-related passwords for personal accounts and vice-versa
    - change a password when there is reason to believe it has been compromised
- Ensuring that all information in electronic form is secure in their work area at the end of the day and when they leave their workspace unattended by:
  - Locking computer workstations
  - Shutting-down computer workstation at the end of the day
- Banking: Complying with 7.3, 7.13, and 7.14 of the Council's Financial Regulations

b) Cyber Security

Cyber Security focuses on securing digital information systems to help protect digital data and assets from cyberthreats. While an enormous undertaking, cybersecurity has a narrow scope as it is not concerned with protecting paper data.

Viruses and malicious software (malware) can infect any computer or device. Most systems have antivirus built in, however, to protect the Council's information assets from threats (whether internal or external, deliberate or accidental) the Council will install additional reputable anti-virus, anti-spyware, and firewall software (as agreed by the Council) on Council owned computers and devices used for the purposes of carrying out Council business, operations, and communications. This software must be regularly updated.

Notwithstanding this, Councillors and Officers must exercise caution with email attachments and links to avoid phishing and malware. Best practice to is verify the source before opening any attachments or clicking on links.

The Council has taken out Cyber Package insurance cover underwritten by Lloyds. This Cyber Package protects the Council from losses, damages, and liabilities that arise following a Cyber Event (as defined in the Cyber Package).

c) Data Resilience

Data Resilience depends on how well an organisation endures or recovers from any type of failure—from hardware problems to power shortages and other events that affect data availability. Speed of recovery is critical to minimise impact.

To ensure the availability of Council data at all times, Councillors and Officers use: -

- Web-based .gov.uk email accounts (password protected) hosted on the Council's owned domain. Hosting support is managed under contract by BWP Creative Limited.
- A cloud-based data storage solution (password protected) accessible from any device. The Council's authorised cloud-based data storage solution is Dropbox; one of the most popular cloud storage solutions in the world. The Council selected Dropbox due to confidence with its security: -
  - 256-bit AES encryption
  - additional security tools like two-factor authentication
  - routinely tests its own hardware, software, and processes for security vulnerabilities
  - alerts users if Dropbox detects an attempted login from a new device or location
  - there have been no known large-scale hacks on Dropbox since 2012.

Repairs to both Council owned and personal computers and devices must be carried out with due consideration to the protection of the confidentiality and integrity of Council data accessed through that computer or device.

The Council has adopted a Risk Management Policy which covers matters pertaining to business continuity.

d) Data Security

To ensure the confidentiality and integrity of data: -

- The Council operates a Clear Desk policy i.e. at the end of the day and when they leave their workspace unattended, Councillors and Officers ensure that all information in paper form is secure by: -
  - removing any restricted or sensitive information from the desk and place in a locked drawer
  - closing and locking filing cabinets containing restricted or sensitive information
  - not leaving keys used for accessing restricted or sensitive information unattended
  - clearing all printers of papers containing restricted or sensitive information
  - upon disposal, shredding restricted and/or sensitive documents
- Councillors and Officers must not discuss confidential information with anyone outside of Council business.

e) Data retention

Full details are set out in the Council's Info and Data Protection and Data Retention Policy.

f) Councillors and Officers: upon leaving the Council

All Council owned computers and devices, passwords for all physical and digital IT assets, and physical papers must be surrendered to the Council's Clerk or Chair. Councillors and Officers will be asked to sign a declaration to confirm compliance.

5. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated Data Protection Officer (the Clerk) for investigation and resolution. Incidents such as a suspected loss, breach, or theft of their computer or device.

The Council is registered as a Data Controller with the Information Commissioner's Office (ICO) Registration Certificate no. Z7511938.

The Clerk must report notifiable breaches to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

6. Awareness

The Council will provide a copy of this Policy to all Councillors and Officers when it is adopted by full council, plus to all new Councillors and Officers as part of their Induction Plan. This Policy will be considered (contents reviewed and for re-adoption) at the Annual Parish Council Meeting held in May each year.

Breach of this Policy through misuse of negligence can lead to serious consequences such as loss of trust, legal action, referral to the Monitoring Officer, disciplinary action, even termination of employment.