HALE PARISH COUNCIL – IT POLICY

Version: 1.0
Adopted: 18th May 2026
Review Date: 18th May 2027
Responsible Officer: The Clerk (Proper Officer)

---

1. INTRODUCTION

IT systems and equipment are fundamental to the effective operation of Hale Parish Council, supporting communication, record-keeping, service delivery and engagement with residents. This document sets out **Hale Parish Council's own formal position and policy** in relation to the use of IT facilities. It has been developed following National Association of Local Councils (NALC) recommendations and reflects current legal obligations including the UK GDPR, Data Protection Act 2018 and relevant statutory regulations.

The aims of this policy are to:

- Establish clear standards and expectations for all users of Council IT systems and equipment;
- Protect confidential data and digital assets;
- Minimise security risks and ensure full compliance with the law;
- Clarify rights, roles and responsibilities whether equipment is owned by the Council or privately owned;
- Provide a consistent framework for all working arrangements, including office-based, home-based and remote working.

---

2. SCOPE

This policy applies to all councillors, staff and authorised users, regardless of working pattern or location. It covers all Council-owned hardware and software, as well as personal devices used to access, store or process Council business or data.

---

3. GENERAL USE OF EQUIPMENT

Council-provided IT equipment and systems are primarily intended for Council business. **Limited, incidental personal use is permitted**, provided that:

- It does not interfere with Council work or disrupt services;
- It is restricted to official break times or outside normal working hours;
- It does not involve any illegal, offensive or reputational risk-related activity;
- It remains reasonable in frequency and duration, as determined by the Proper Officer.

3.1 Hardware

- All equipment is issued for the performance of Council duties and must be treated with care at all times.
- Computers must be locked whenever the user leaves their desk to prevent unauthorised access – this applies to both Council-owned and personal devices used for work purposes. Failure to comply may result in disciplinary action.
- Equipment must be kept clean and protected from spills, dust or physical damage.
- Each item will be individually numbered and recorded in a central equipment register, showing the current user and location.
- No equipment is to be dismantled, modified or repaired without prior consultation with the Proper Officer.
- No equipment, software or digital services may be purchased on behalf of the Council without written authorisation from the Proper Officer or Council Chair.
- Personal storage devices (USB sticks, external drives, CDs/DVDs etc.) must not be connected to Council computers unless approved in advance by the Proper Officer.
- Users are prohibited from creating personal Wi-Fi hotspots to bypass the Council's secure network.
- Any fault, damage or security concern must be reported immediately to the Proper Officer.

  3.2 Portable Equipment

  Portable equipment includes laptops, tablets, smartphones and any device capable of storing or transmitting Council data.
- All portable devices must be protected by a PIN, password or biometric lock. Where available, devices should be set to wipe data after multiple unsuccessful login attempts. Security features must never be disabled or removed.
- Two-Factor Authentication (2FA) will be enabled wherever technically possible to add an extra layer of protection.
- When not in use, devices should be stored securely. When travelling or working remotely, they must remain with the user or kept in a locked secure location. Under no circumstances should portable equipment be left unattended in vehicles or unsecured premises.
- If a device is lost, stolen or damaged, this must be reported to the Proper Officer immediately. Where loss or damage is due to negligence, the user may be required to contribute towards the cost of replacement or repair.
- Taking photographs or video recordings on Council premises is prohibited unless authorised in writing by the Council, and only where necessary for official business.
- No meeting or conversation (other than those held in public under the *Openness of Local Government Regulations 2014*) may be recorded without the prior consent of all those present.

- Webcams (whether built-in or external) may only be used for Council-related conference calls or meetings, and only where the device is located in a suitable environment. Advice on appropriate use should be sought from the Proper Officer if in doubt.

---

4. BACK-UP ARRANGEMENTS

To safeguard Council data and ensure business continuity:

- All official records and documents stored on Council systems will be backed up automatically on a **daily basis** to secure off-site storage.
- Users must ensure that work files are saved to designated Council network drives or approved cloud storage – not to local device hard drives – to ensure they are included in the backup routine.
- Portable devices and personal devices used for Council work are not part of the Council's automated backup system; users are responsible for transferring completed work to Council storage promptly. The Proper Officer can provide guidance on how to do this securely.
- Backup data will be retained in line with the Council's Records Management and Publication Schedule.

---

5. EMAIL AND DATA PROTECTION RESPONSIBILITIES

- All Council business must be conducted using an official Council email address provided by Hale Parish Council. Personal email accounts must never be used for Council business, nor should Council emails be set to auto-forward to personal accounts.
- **Hale Parish Council is the Data Controller** for all information held or communicated through official systems.
- All users act as **Data Processors** on behalf of the Council and are required to handle personal data in accordance with the UK GDPR, Data Protection Act 2018 and the Council's separate Data Protection Policy.
- Councillors do not act as independent Data Controllers in relation to Council business; legal responsibility remains with the Council as a corporate body.
- All email communications form part of the Council's official records and may be retained, archived or disclosed in accordance with statutory requirements.

---

6. BRING YOUR OWN DEVICE (BYOD)

Where users choose to use personal phones, tablets or computers for Council purposes, the following rules apply:

6.1 Minimum Standards

- Devices must be protected by a PIN, strong password or biometric security.

- Operating systems, antivirus and security software must be kept up-to-date at all times.
- Council data and communications must be kept clearly separate from personal content, for example by using separate user profiles or dedicated applications.
- Wherever possible, work-related data should be stored on Council systems rather than on the personal device itself.

6.2 Retrieval and Deletion of Data

- When leaving the Council or upon request, users **must cooperate fully with reasonable steps** required to secure, retrieve, preserve or permanently delete Council data held on their personal device.
- The Council will seek to avoid accessing or handling personal data unless it is strictly necessary and proportionate to meet legal or operational requirements. Legal advice will be sought where there is uncertainty or complexity.
- Following termination of service or office, all Council-related emails, files and contacts must be removed from the device immediately.

6.3 Additional Safeguards

- Confidential documents sent by email must be password-protected, with the password sent separately via a different communication channel.
- Only secure, trusted Wi-Fi networks should be used when accessing Council systems.
- Users must ensure that Council data cannot be viewed or accessed by family members or other users of the device.
- If a device is lost, stolen or subject to unauthorised access, the Proper Officer must be informed without delay, and details such as IMEI or SIM numbers provided where possible to assist in protection of Council data.
- Personal cloud storage services must not be used to store Council data, as this may breach data protection law and security standards.
- When transferring data via removable media, the information must be securely deleted from the device once the transfer is complete.
- Any cached copies of documents or emails must be deleted immediately after use.

---

7. WEBSITE STANDARDS

- **Accessibility:** The Council website will be designed and maintained to meet the **WCAG 2.2 AA** standard, ensuring it is usable by everyone, including people with disabilities.
- **Documents:** All documents published on the website (such as agendas, minutes and reports) will be produced in formats compatible with assistive technology such as screen readers.

- **Accessibility Statement:** A formal Accessibility Statement will be published and reviewed annually to ensure it remains accurate and up-to-date.

---

8. PASSWORD AND AUTHENTICATION POLICY

- All user accounts must be protected by strong passwords, following National Cyber Security Centre (NCSC) guidance – ideally using three random words (e.g. *PurpleCandleRiver*), which are both secure and memorable.
- Multi-Factor Authentication (MFA) will be enabled wherever possible, adding a second form of verification such as a code sent to a registered mobile device.
- Initial passwords for new accounts will be generated by the Proper Officer or nominated IT provider and must be changed immediately upon first use.
- Default passwords provided by software vendors must always be changed immediately following installation.
- Passwords are personal and must never be shared or disclosed to others.
- Administrative passwords will be stored securely and held in a sealed envelope with the Council Chair, accessible only in an emergency and subject to formal recording.
- Passwords must not be written down or stored in plain text; only approved encrypted password managers may be used.
- Passwords must be changed immediately if compromise is suspected.
- All access to administrative or shared credentials will be logged and auditable; unauthorised attempts will be treated as security incidents.
- Users are responsible for maintaining the security of their own credentials; the Proper Officer is responsible for system-level security and policy enforcement.

---

9. MONITORING AND RETENTION OF RECORDS

The Council reserves the right to monitor IT usage proportionately and in line with the *Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018* and UK GDPR. Monitoring will only be carried out where there is a legitimate purpose, and all users are informed that such activity may take place.

9.1 Retention Periods (in line with Council's Records Management and Publication Schedule)

- Internet usage logs, email metadata and system activity records: retained for **12 months**, then securely deleted or anonymised.
- Security incident logs and audit trails: retained for **3 years**.
- All other records: retained in accordance with statutory and best-practice timescales as detailed in the Schedule.

9.2 Responsibility for Monitoring and Audit

Overall responsibility for the implementation, monitoring and enforcement of this policy rests with the **Proper Officer (The Clerk)**. Their duties include:

- Conducting a **formal review and audit of systems, security settings and compliance** at least **once every 6 months**;
- Carrying out ad-hoc checks where concerns are raised or incidents occur;
- Maintaining clear records of audits and any follow-up actions taken;
- Providing guidance, training and updates to users as required;
- Reporting annually to Council on policy compliance and recommending any necessary updates or changes.

---

10. REMOTE WORKING – LOGGING IN AND SECURITY

The requirements below apply when accessing Council systems from any location outside the Council's main premises, including when working from home, travelling or using public Wi-Fi. These rules apply to **all Council systems and services**, including:

- Network files and shared drives;
- Council email accounts;
- Cloud-based applications and databases;
- Any other platform containing Council data or records.

10.1 Remote Working Rules

- If using a device not owned or managed by the Council, passwords must never be saved in browsers or applications, and the user must fully log out at the end of each session. All browsing history, cache and temporary files must be deleted immediately afterwards.
- If the security or reliability of the device or network cannot be guaranteed (for example in an internet café or public hotspot), Council systems must not be accessed.
- Screens must be positioned so that confidential information cannot be overlooked by others; privacy filters should be used when working in public places or shared spaces.
- Printed documents must be collected immediately and stored securely or disposed of confidentially when no longer required.
- Paper files or storage devices must never be left unattended in vehicles unless unavoidable, in which case they must be locked in the boot and removed as soon as possible. Overnight accommodation must be secure and documents kept safe from access by third parties.
- Where technically feasible, the Council retains the ability to remotely wipe mobile devices containing sensitive data in the event of loss or theft.

- Devices issued with 3G/4G/5G dongles should be used only for essential Council business, particularly when abroad or roaming, due to potential high costs.
- Paid-for Wi-Fi services should be used sparingly and only where necessary to complete urgent work.

---

11. HEALTH AND SAFETY

- All office-based users will be provided with a suitable workstation arranged to meet health and safety requirements.
- The Council will arrange regular eye tests for employees who use display screen equipment, in line with legal requirements – details are available in the Staff Handbook.
- Any concerns regarding workstation set-up, equipment noise, or other hazards must be reported immediately to the Proper Officer.

---

12. INTERNET USE AND COPYRIGHT

- All use of the internet must comply with the law and this policy.
- Much material on the internet is protected by copyright under the *Copyright, Designs and Patents Act 1988*. Copying, downloading or distributing material without permission is illegal and strictly prohibited.
- Users should not assume that information in the public domain is free from copyright restrictions.
- Copyright warnings and terms of use published on websites must be respected.
- If in doubt about whether material may be used or reproduced, advice should be sought from the Proper Officer.
- No new domain names or trademarks may be registered in the name of the Council without express approval.
- Links from Council websites to external sites must be checked and approved by the Proper Officer before publication.
- Users should be aware that information found online may be inaccurate or out of date; verification from reliable sources is essential before use or publication.

---

13. USE OF SOCIAL MEDIA

Social media includes social networks, blogs, video-sharing platforms, forums, messaging apps and similar services. These rules apply both when using Council systems and when using personal devices or accounts, whether during or outside working hours.

13.1 Standards of Conduct

- Personal use should be restricted to break times or outside working hours.

- Use for Council purposes is encouraged where it supports engagement, communication or the Council's aims – but it must always be professional, accurate and respectful.
- Any content which could reasonably be linked to the Council, or which refers to the Council, its work, staff or members, must not be offensive, abusive, discriminatory, defamatory or likely to damage the Council's reputation.
- Where a user identifies themselves as a councillor or employee in an online profile or post, they must clearly state that any personal views expressed are their own and do not represent the views of the Council. A suitable disclaimer must be included.
- Users must not claim to speak on behalf of the Council without prior written authority.
- Proposed blogs, websites or social media accounts which will mention or represent the Council must be approved by the Proper Officer before being launched.
- Contact details from Council databases must not be uploaded or synchronised with social media address books unless authorised.
- Images or videos showing Council uniforms, branding or premises must not be posted if they could reflect adversely on individuals or the Council.
- Internal discussions, confidential business or personal data about councillors, staff, contractors or residents must never be shared online.
- Users are personally liable for what they post and should be aware of the Council's *Code of Conduct* and the *Nolan Principles* in all online activity.
- Enquiries from the media should always be referred to the Proper Officer.
- Upon leaving the Council, users must update their online profiles to remove references to their role and must delete all Council-related contacts and data from personal accounts or devices.
- Council-managed social media accounts must have login details held securely by the Proper Officer so that access can be maintained if the responsible user leaves.
- Former members or staff must not post material that is detrimental to the Council or its reputation.
- All professional contacts developed or maintained in the course of Council duties remain the property of the Council and must be disclosed or deleted as required when leaving office or employment.
- The Council reserves the right to monitor publicly available social media posts where there is reason to believe this policy may have been breached.

---

14. MISUSE AND ENFORCEMENT

Misuse of IT systems, equipment or data is regarded as a serious matter and is inconsistent with the Council's standards of conduct. Breaches of this policy may result in:

- Formal investigation;

- Restriction or removal of IT access;
- Disciplinary proceedings, up to and including dismissal for staff;
- Referral to the Monitoring Officer or Standards Committee for councillors;
- Legal action where there has been a breach of law or confidentiality.

---

15. GUIDANCE AND SUPPORT

If any user is unsure about the application or interpretation of this policy, they should seek advice from the Proper Officer before taking action. Guidance and training will be provided as necessary to ensure understanding and compliance.
