Hallow Parish Council
Information Technology (IT) Policy
Based on the NALC / CALC Model IT Policy
Adopted: January 19th 2026
Signed by Chair: Hazel Kemshall
Review date: January 2029

---

1. Introduction

Hallow Parish Council recognises the increasing role of information technology in the effective administration of the Council's activities. This policy sets out the framework for the secure, lawful and appropriate use of IT systems and electronic communications by councillors, employees and others acting on behalf of the Council.
This policy supports compliance with **AGAR Annual Governance Assertion 10**.

---

2. Scope

This policy applies to:

- All councillors
- The Clerk and any other employees
- Any person authorised to use Council IT systems or access Council data

---

3. Legal Framework

This policy is informed by, and must be read in conjunction with:

- Data Protection Act 2018 and UK GDPR
- Freedom of Information Act 2000
- Local Government Act 1972
- Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018
- Relevant guidance issued by NALC and CALC

---

4. IT Systems and Equipment

- IT equipment and systems used for Council business must be appropriate, secure and maintained.
- Where personal devices are used for Council business, users must ensure that reasonable security measures are in place.
- Council information must not be stored on shared or unsecured devices.

---

5. Email and Electronic Communications

- Council business must be conducted using **Council-controlled email accounts**.
- Personal email accounts must not be used for official Council correspondence.
- Users should be aware that electronic communications may be subject to **Freedom of Information requests** and audit inspection.
- Emails should be managed in accordance with the Council's document retention arrangements.

---

6. Data Protection and Information Security

- Personal data must be processed lawfully, fairly and securely.
- Access to data must be restricted to those who need it for Council purposes.
- Passwords must be kept secure and not shared.
- Any actual or suspected data breach must be reported immediately to the Clerk.

---

7. Website and Accessibility

- The Council will maintain an official website to publish information required by law.
- The website will be maintained in accordance with **accessibility regulations**, and an Accessibility Statement will be published and kept under review.
- Information required under the **Transparency Code for Smaller Authorities** will be published and kept up to date.

---

8. Software, Cloud Services and Backups

- Only authorised software and cloud-based services may be used for Council business.
- Appropriate backup arrangements will be in place to protect Council data.
- Cloud service providers must offer suitable security and data protection safeguards.

---

9. Acceptable Use

Users must:

- Use IT systems only for legitimate Council purposes
- Not install unauthorised software or access inappropriate content
- Take reasonable steps to protect Council systems from cyber risks

---

10. Training and Awareness

- Councillors and employees will be made aware of this policy and their responsibilities.
- New councillors will receive appropriate guidance as part of their induction.

---

11. Review and Monitoring

- This policy will be reviewed annually or when required by changes in legislation or guidance.
- Compliance with this policy is the responsibility of all users.
