WINDLESHAM PARISH COUNCIL
IT POLICY

Table of Contents

Table of Contents

Version & Date	Amendments made
V1.0-251108	Adopted at the Full Council Meeting held on the 25th November 2025

1 Introduction

Windlesham Parish Council recognises the importance of secure and compliant IT practices in line with the SAAA Practitioners' Guide Assertion 10 and the NALC Information Technology Policy Guidelines. This policy sets out mandatory requirements for IT, email, and data governance.

2 Scope

This policy applies to all councillors, employees, volunteers, and contractors using Windlesham Parish Council IT resources, including computers, networks, mobile devices, telephones, and the council website.

3 Related Policies

This policy should be read in conjunction with the Council's Data Protection Policy, Disciplinary Policy, Equality and Diversity Policy, and any other relevant policies.

4 Responsibility & Monitoring

The Clerk (or designated IT lead) is responsible for monitoring and reviewing this policy, supporting staff understanding, and enforcing compliance. The Council reserves the right to monitor IT and email usage for legitimate reasons, and staff will be informed of this.

5 Council Owned Domain & Email

-All official email addresses must use a Windlesham Parish Council-owned domain (e.g., @windleshampc.gov.uk or .org.uk).

-Free email services (Gmail, Hotmail, etc.) are prohibited for council business.

-Domain and email accounts must be managed securely with continuity plans.

6 Website Accessibility

The Windlesham Parish Council website must comply with WCAG 2.2 AA standards.

An accessibility statement must be published and maintained.

7 Acceptable Use & Personal Use

IT resources and email accounts are for official council business.

Limited personal use is permitted if it does not breach this policy. All use (including personal) may be monitored.

8 Password & Account Security

Strong passwords are required and must not be shared.

Multi-factor authentication should be enabled where possible.

If a password is compromised, it must be reported and changed immediately.

If access to another employee's system is required (e.g., due to absence), this must be authorised by the Clerk.

9 Computer Usage & Security

Computers must be shut down at the end of each day.

Users should log out when leaving their desks.

Documents should be saved in secure, backed-up locations.

Extra precautions must be taken in areas with public access.

10 Bring Your Own Device (BYOD)

Personal devices may only be used for council work with prior written approval and must comply with all council security requirements.

11 Data Protection & GDPR

All data handling must comply with UK GDPR and the Data Protection Act 2018.

The six data protection principles must be followed for collecting, storing, retaining, using, disclosing, and disposing of personal information.

Sensitive data must be encrypted in transit and at rest.

12 Mobile Phones & Texting

Work-related texting is permitted only for official purposes and must not contain illegal or discriminatory content.

Abbreviations should be avoided in official communications.

13 Email Communication

Emails must be professional and respectful.

Sensitive information must be encrypted.

Attachments and links must be verified before opening.

Staff must not enter into agreements with suppliers via email without proper authority.

14 Internet Use

The internet is to be used for council business.

Accessing inappropriate content, chat rooms, or unauthorised messaging services is prohibited.

A firewall is in place to protect council systems.

15 Software

Only authorised software may be installed on council devices.

Downloading or installing unauthorised software is prohibited.

16 Training & Awareness

All staff and councillors will receive regular training on IT security, GDPR, accessibility, and best practices, including induction training for new starters.

17 Misuse & Disciplinary Action

Misuse of IT facilities (including policy breaches, attempting to discover another user's password, circumventing security, or deliberate damage) may result in disciplinary proceedings.

18 Incident Reporting

All suspected security breaches or incidents must be reported immediately to the Clerk or designated IT contact.

19 Policy Review

This policy will be reviewed annually and updated as necessary.

20 Compliance Statement

This policy ensures compliance with Assertion 10 of the SAAA Practitioners' Guide and the NALC Information Technology Policy Guidelines. Breaches may result in disciplinary action and audit reporting.