IT and Communications Policy

Adopted: [14th April 2026] | **Review Date:** [April/May 2028]

1. Introduction and Purpose

This policy sets out the standards for the use of Information Technology (IT) resources by Crowhurst Parish Council. It aims to protect the Council's data, ensure legal compliance (UK GDPR/DPA 2018), and maintain the professional reputation of the Council.

2. Scope

This policy applies to all Councillors, the Clerk, and any contractors or volunteers (hereafter "Users") accessing Council systems or handling Council data.

3. Acceptable Use of IT Resources

· **Official Business:** Council IT resources and email accounts must be used for official Parish Council business.

· **Personal Use:** Minimal personal use is permitted, provided it does not interfere with Council duties, incur costs, or breach any security protocols.

· **Prohibited Content:** Users must not access, store, or transmit material that is offensive, defamatory, discriminatory, or illegal.

4. Email and Communication Standards

· **Official Addresses:** All Council correspondence must be conducted via the official @crowhurstparishcouncil.gov.uk email addresses. **Personal email addresses must not be used** for Council business.

· **Professionalism:** Emails are public records and may be subject to Freedom of Information (FOI) requests. They must be professional and respectful.

· **Sign-off:** All emails must include the standard Council disclaimer and contact details.

5. Data Management and Security

· **Storage:** Council documents should be stored in the approved cloud

environment (e.g., Microsoft 365/OneDrive). Storing sensitive data solely on local hard drives or unencrypted USB sticks is prohibited.

· **Passwords:** Users must use strong, unique passwords (at least 12 characters including symbols). Multi-Factor Authentication (MFA) must be enabled where available.

· **Data Breaches:** Any suspected loss of data or unauthorized access must be reported to the Clerk (Data Controller) immediately. Under the *Data Use and Access Act 2025*, the Council must acknowledge data-related complaints within 30 days.

6. Device Security (Including BYOD)

· **Locking:** Devices must be "screen-locked" when left unattended.

· **Software:** Only Council-approved software may be installed on devices used for Council business.

· **Updates:** Users are responsible for ensuring that any personal devices used for Council work (Bring Your Own Device - BYOD) have up-to-date anti-virus software and operating system patches. ·

7. Social Media

· **Representation:** Only authorized individuals may post on behalf of Crowhurst Parish Council.

· **Personal Accounts:** Councillors should make it clear that views expressed on personal accounts are their own and do not necessarily reflect the Council's position.

8. Compliance and Consequences

Failure to comply with this policy may result in the suspension of IT privileges or, for employees, disciplinary action. For Councillors, breaches may be referred under the Code of Conduct.

Implementation Checklist for the Clerk

Task	**Status**
Ensure all Councillors have an active @crowhurst.gov.uk email.	[ ]
Verify MFA (Multi-Factor Authentication) is active for all users.	[ ]
Add "IT Policy Review" to the Annual Meeting agenda.	[ ]
Update the Council's Privacy Notice to reflect 2026 complaint procedures.	[ ]

Review Date: March 2028