Information Technology (IT) and Data Usage Policy

1. Introduction and Scope 1
2. General Principles & Security 1
3. Data Management and Protection (GDPR Focus) 2
4. Email and Internet Use 3
5. Mobile Devices and Remote Working 3
6. Consequences of Breach 4

1. Introduction and Scope

1.1 Purpose To define the acceptable and secure use of Hullavington Parish Council's Information Technology (IT) resources by all Councillors, employees (e.g., the Clerk/RFO), and contracted third parties.

1.2 Scope This policy applies to:

- **All Users:** Councillors, the Clerk/RFO, and any volunteers or contractors using Council resources.
- **All IT Resources:** Council-provided computers, laptops, tablets, smart devices, networks, email accounts, cloud storage (e.g., SharePoint, OneDrive, Councilapproved cloud services), and the Parish Council Website.
- **Council Data:** Any information relating to Council business, regardless of where it is stored (paper or electronic).

2. General Principles & Security

All users must act responsibly and professionally to protect the Council's IT assets and data.

Principle	Detail
Official Use	Council IT resources are primarily for official Parish Council

Principle	Detail
	business. **Limited, reasonable** personal use is permitted, provided it does not interfere with duties, incur a cost to the Council, or violate any other part of this policy.
Passwords	Passwords must be **strong** (a mix of letters, numbers, and symbols) and changed regularly. **Passwords must never be shared** or written down where others can find them.
Anti-Virus/Security	All Council-provided devices must have up-to-date antivirus/security software running at all times. Users must not disable or circumvent these measures.
Unauthorised Access	Users must not attempt to access any data, files, systems, or websites they are not authorised to use.
Reporting Incidents	Any suspected security breach, virus, phishing attempt, or loss/theft of a Council device must be reported immediately to the Clerk and Chair.

3. Data Management and Protection (GDPR Focus)

The Council is a **Data Controller** for the personal data it holds. All users must comply with the Data Protection Act 2018/GDPR.

Area	Requirement
Data Storage	All Council data, especially confidential and personal data, **must be stored on Council-approved systems** (e.g., a secure, backed-up cloud drive or server). **Data must never be saved only to a local device** (e.g., a desktop or personal laptop hard drive).
Personal Data	Personal data (e.g., names, addresses, emails) must be handled only for the purpose for which it was collected (as outlined in the Council's Data Protection Policy).
Data Security	Files containing confidential or sensitive personal data must be **password protected or encrypted** before being sent externally via email.
Retention	Data must be retained or destroyed according to the Council's **Document Retention and Disposal Policy**.

4. Email and Internet Use

4.1 Email Communication

- **Official Accounts:** Councillors and the Clerk/RFO will be issued a Council email address (e.g., clerk@hullavingtonpc.gov.uk). This account **must be used for all Council business.**
- **Professionalism:** All emails must be professional in tone and language, as they are a formal written record of the Council's business.
- **Confidentiality:** Confidential or sensitive information should not be sent via unencrypted email. Do not forward Council email to a personal, non-Council email account.
- **Retention:** Emails related to Council business are formal records and may be subject to the Freedom of Information Act (FOIA) or Data Subject Access Requests.

4.2 Internet Use (Acceptable/Unacceptable)

Acceptable Use (for Council Business)	Unacceptable Use (Strictly Prohibited)
Researching local government guidance.	Accessing, creating, or downloading obscene, offensive, or discriminatory material.
Communicating with residents, suppliers, and external bodies.	Creating or sending defamatory or libellous statements.
Updating the Council website/social media.	Downloading pirated or copyrighted material (e.g., software, music, films).
Using Council resources to pay invoices or conduct online banking.	Gambling, personal trading, or engaging in extensive personal shopping.

5. Mobile Devices and Remote Working

- **Council-Owned Devices:** Devices (laptops, phones) must be locked with a passcode/biometric authentication. They must be kept secure and never left unattended in public places or visible in vehicles.
- **Personal Devices (BYOD - Bring Your Own Device):** If a user accesses Council email or documents on a personal device, that device **must be password protected** and the user must agree that the Council has the right to access and

delete Council data on that device if necessary (e.g., if the device is lost or the user leaves office).

6. Consequences of Breach

Any breach of this IT policy may be treated as misconduct and could lead to:

- Immediate suspension of access to Council IT resources.
- Disciplinary action (for employees) or referral to the Standards Committee (for Councillors).
- Legal action against the individual or the Council if the breach results in a data loss or violation of law (e.g., Data Protection Act, Computer Misuse Act 1990).

Date of policy: 11th November 2025

Approving committee: Ordinary Council Meeting

Date of meeting: 11th November 2025

Supersedes: N/A

Policy effective from: Immediate

Date for next review: November 2026