KILMINGTON

PARISH COUNCIL

INFORMATION TECHNOLOGY & EMAIL ACCEPTABLE USE AND SECURITY

POLICY

1. Purpose and compliance

Kilmington Parish Council recognises that secure and effective information technology (IT) and email are essential to its operations, decision-making, public engagement, and legal obligations. This policy sets out mandatory rules for using Council IT systems and email, to:

- Protect the confidentiality, integrity, and availability of Council information and systems.
- Demonstrate effective internal controls as required by **AGAR Assertion 10**.
- Comply with **UK GDPR**, the **Data Protection Act 2018**, the **Freedom of Information Act 2000**, and other applicable laws and guidance (including the Local Government Transparency Code).
- Promote good practice aligned to **Cyber Essentials** where proportionate.

.

2. Scope

This policy applies to **all users** who access Council information or systems, including:

- Councillors, employees, volunteers, contractors, and third parties.
- All Council IT resources and information, including computers, mobile devices, networks, software, cloud services (e.g. Microsoft 365/OneDrive), email accounts, and data in any form.
- **Personally owned devices** (BYOD) when used for Council business, where expressly authorised and enrolled in Council security controls.

3. Roles and responsibilities

- **The Council (Data Controller):** Responsible for overall compliance, risk management, and internal controls.
- **Parish Clerk (Proper Officer):** Acts on behalf of the Data Controller as the Data Protection Lead; coordinates information governance, access control, incident management, training, and oversight
- **Users:** Must comply with this policy and complete required training. Users are personally responsible for safeguarding Council information and reporting incidents promptly.

4. Acceptable use of IT resources and email

Council IT resources and email are for **official Council business**. Limited personal use is permitted where it:

- Is lawful, reasonable, infrequent, and does not interfere with duties.
- Does not incur cost or reputational risk to the Council.
- Does not breach any part of this policy.

Strictly prohibited uses include (non-exhaustive):

- Accessing, creating, storing, or sharing illegal, offensive, or discriminatory content.
- Political campaigning or personal commercial gain using Council systems.
- Excessive personal use or personal cloud/email accounts for Council records.

Adopted on: 11 May 26

- Bypassing security controls, using peer-to-peer/file-sharing tools, or introducing malware.
- Copying or using software or content without proper licence or permission.

5. Information classification and handling

Council information must be handled according to its sensitivity:

- **Public:** Intended for public disclosure.
- **Internal:** Routine Council business not for general publication.
- **Confidential/Personal:** Personal data, commercially sensitive, or otherwise confidential.
- **Restricted (Special Category/Highly Sensitive):** Special category personal data, security-sensitive, or legally restricted.

Minimum handling rules:

- Store all Council information only in **approved systems** (e.g. OneDrive/Teams or approved shared drives).
- Do **not** use personal email, messaging apps, or personal cloud storage for Council business.
- Encrypt **in transit and at rest** where supported; use password protection for sensitive files when sharing, and share via approved secure links, not as open attachments.
- Apply data minimisation—keep only what is necessary, accurate, and up to date.
- Follow the Council's **Records Management & Retention Schedule** (see section 13).
- Physical records (printouts, notebooks, memory sticks) must be stored securely and disposed of using **secure destruction** methods (e.g., cross-cut shredding or approved confidential waste).

6. Access control, passwords, and MFA

- **Individual accounts only;** account sharing is prohibited.
- Grant the **least privilege** necessary; remove access promptly when no longer required.
- **Passwords:** Minimum 12 characters, use passphrases where possible, avoid reuse, and never share or write down in plain text.
- **Multi-Factor Authentication (MFA):** Mandatory on all systems where available (e.g., Microsoft 365).
- Lock devices when unattended and log out at the end of use.
- Suspected compromise must be reported **immediately** (see section 14).

7. Devices and software (including BYOD)

- Council-owned devices will be configured with:
    - Supported operating systems; automatic security updates; disk encryption; device firewalls; and reputable anti-malware.
    - **Mobile Device Management (MDM)** for configuration, compliance checks, and remote wipe.
- **Software installation** Users must not install unapproved applications, plug-ins, or browser extensions.
- **Removable media** (USB drives) must be avoided unless expressly authorised; if used, they must be encrypted and scanned.
- **BYOD (if authorised):** Must be enrolled into MDM, protected by a device passcode/biometric, up-to-date, and subject to remote wipe of Council data.

8. Network and internet use

- **Public Wi-Fi:** Do not access confidential/personal data on public Wi-Fi unless using an approved **VPN**.
- Never circumvent security controls, change network settings, or connect unauthorised hardware.
- Only use **approved file transfer** methods; do not use personal messaging or consumer file-sharing services.

9. Email use

- Council-issued email accounts **must be used for all Council business**.
- **Auto-forwarding to personal accounts is prohibited.**
- Maintain a professional tone; treat email as a formal record that may be disclosed under FOI or in legal proceedings.
- **Sensitive/confidential content:** Use encryption/secure sharing links; verify recipients; avoid sending sensitive data in the email body.
- Be vigilant against phishing and malware:
    - Check sender identity, links, and attachments; when in doubt, do not click.
    - Report suspicious emails immediately.
- Archive and file emails in line with section 13; keep your mailbox manageable and orderly.

10. Remote working

- Use secure, private working environments; prevent viewing by others; use privacy screens if appropriate.
- Store Council data only in approved systems; avoid local downloads unless necessary and then promptly move to approved storage.
- Do not allow family or other third parties to use Council devices or access Council information.
- Lost or stolen devices must be reported **immediately** for remote lock/wipe.

11. Monitoring and privacy notice

To protect systems, data, and public funds, the Council may **monitor and audit** the use of IT systems and email (including logs, traffic, and content) for legitimate purposes such as security, compliance, and investigation of misconduct.

Monitoring will be **proportionate** and in accordance with applicable law (including UK GDPR and the Data Protection Act 2018). Users should have **no expectation of privacy** when using Council systems.

12. Third-party access

- Contractors with access to Council systems/data must comply with this policy and UK GDPR.
- Access for third parties must be **time-limited**, **role-based**, and removed when no longer required.

13. Records, retention, and archiving

- Emails and documents that form part of Council business are **records** and must be filed in the designated repository (e.g. OneDrive/approved filing system).
- The Council's **Records Management & Retention Schedule** governs how long records are kept and how they are disposed of.
- Email is generally **transitory**—move the content of record to the appropriate file and delete the redundant email.
- Retention supports compliance with the **Freedom of Information Act 2000**, **UK GDPR** (storage limitation), and transparency duties.
- Destruction must be **secure** and documented where appropriate.

14. Security incident and data breach reporting

All users must report suspected or actual security incidents **immediately** (and no later than **24 hours**) to the **Parish Clerk**. Examples include:

- Lost or stolen devices; suspected account compromise; malware infection; mis-sent emails; unauthorised access or disclosure; denial-of-service; physical break-ins.

Do not investigate beyond isolating the issue (e.g., disconnect network, power down if instructed). The Clerk will coordinate investigation and, where personal data is involved, assess reporting to the **ICO within 72 hours** if required and notify affected individuals where applicable. All incidents will be logged.

Adopted on: 11 May 26

15. Training and awareness

- **Mandatory induction** training for all councillors, employees, and regular volunteers.
- **Annual refresher** training covering phishing awareness, data protection, secure handling, and incident reporting.
- Additional, role-based training for those with elevated access.

16. Compliance and enforcement

Failure to comply with this policy may result in:

- Suspension or withdrawal of IT access.
- Investigation under relevant HR policies for staff, or Codes of Conduct for councillors.
- Referral to the Monitoring Officer and/or external authorities (e.g., ICO) where appropriate.
- Contractual remedies for contractors.

Serious breaches may constitute misconduct or gross misconduct and could lead to civil or criminal liability.

17. Policy management

- **Ownership:** Parish Clerk (Proper Officer).
- **Approval:** Full Council.
- **Review:** At least **annually**, or sooner following significant changes in law, technology, risk, or incidents.
- **Related policies:** Records Management & Retention Schedule, Codes of Conduct, Disciplinary Policy, Data Protection Policy.

18. Contacts

Primary contact: Steven Willis|+447917842297|clerk@kilmingtonwiltshireparishcouncil.gov.uk

Adopted on: 11 May 26