Ilmington Parish Council

Information Technology Policy

1. Purpose

   Ilmington Parish Council ('the Council') recognises the importance of computer systems and email in supporting its business, operations, and communications, and the need to safeguard the Council's digital data and assets.

   This policy sets out expectations for the responsible use of IT and provides guidance to help councillors and employees use systems safely and securely.

2. Scope

   It applies to all individuals who use the computer systems and email provided by the Council, regardless of their working pattern or location, including those who are home-based or office-based, flexible or part-time, councillors or employees.

3. Cyber security responsibilities

   Responsibility for the administration of the Council's IT systems, has been delegated to the Clerk, either directly or through an authorised IT provider. The Council remains ultimately accountable for compliance with this policy.

   The Council aims to manage its IT systems in accordance with the principles set out in NCSC Cyber Essentials Guidance and the 2025 Practitioners' Guide.

   For further information see: Cyber Essentials: Overview

4. Acceptable use of IT equipment and email

   Council IT equipment and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy.

   All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

5. Computer and software usage

   Employees who need to use IT in their role will be provided with authorised, licensed computer equipment, software, and applications for work-related tasks.

   All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

   All computers and other devices supplied should be treated with good care at all times, to avoid loss or damage that would have a financial impact on the Council.

The installation of any unlicensed software on council devices is strictly prohibited.

All devices, including computers, laptops, and mobile phones must be kept up to date with security patches. Automatic updates should be enabled where possible, or devices should be patched on a regular schedule.

Regular data backups of Council devices should be performed to allow for a prompt recovery of essential services following a cyber security incident. Backups should be stored separately from live systems (ideally off-site or in a secure cloud) so that data is protected even if primary systems are compromised.

6. Email communication

All councillors and employees who need to use email as part of their role will normally be given their own email address and account on a domain owned by the Council.

Email accounts provided by the Council are for official communication only. Emails should be professional and respectful in tone, and not contain material that could bring the Council into disrepute.

Councillors are strongly encouraged to use their Council-provided email account for official business so that Council data remains secure and under Council control. Using personal email should be limited and only when absolutely necessary.

To reduce the risk of phishing and other email threats, users should take the following precautions:

- **Be cautious of unexpected or unusual emails**, particularly those asking you to click a link, open an attachment, or provide information.
- **Check the sender's email address carefully**, not just the display name. Fraudulent emails often imitate familiar names but use incorrect or unusual addresses.
- **If an email seems suspicious, do not reply, click links, or open attachments.** Forward suspicious emails to report@phishing.gov.uk.
- **Do not trust urgent or threatening wording**, as this is often a sign of phishing attempts.

7. Password and account security

All user accounts must be protected by strong, secure passwords. The National Cyber Security Centre (NCSC) approach of using three random words (e.g. PurpleCandleRiver) is recommended. This method helps create passwords that are both strong and easy to remember, while offering effective protection.

In addition to strong passwords, Multi-Factor Authentication (MFA), e.g. a code to a mobile phone, should be enabled wherever possible.

Additional requirements:

(a) Default passwords must be changed immediately upon installation or setup.
(b) Passwords are personal and must not be shared under any circumstances.
(c) Passwords must not be stored in plain text or written down in insecure locations.
(d) Passwords must be changed immediately if compromised.

Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chairman of the Council, in a sealed envelope, only to be accessed in an emergency.

8. Retention and archiving

   Electronic records should be managed in accordance with the council's Document Retention Policy. Where records contain personal data they should be securely destroyed at the end of the retention period as outlined in the policy.

9. Personal devices

   The Council recognises that employees may wish to use their own smartphones, etc for normal council purposes, including, but not limited to, reading their emails, or using cloud-based Council apps or accounts. Any such use of personal devices will be at the discretion of the Council, but consent will normally be permitted.

   Personal devices should be secured with strong passwords in accordance with the previous section, and biometric authentication where available.

   Personal devices should be kept up to date with security patches.

   Wherever possible the user should maintain a clear separation between data processed on the Council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

   In cases of legal proceedings, the Council may need to temporarily take possession of a device, whether Council-owned or personal to retrieve the relevant data.

10. Secure remote working

    When working away from the normal place of work the following applies:

    (a) Avoid using public or insecure Wi-Fi for confidential Council business.
    (b) Ensure portable devices have encryption enabled.
    (c) If leaving portable equipment unattended is unavoidable, it must be kept in a locked room or cabinet, or secured in the boot of a car for a short period.
    (d) When logging into the Council's systems remotely, using computers that do not belong to the Council or the user, do not save any passwords, log out at the end of the session and delete all logs and browser history. If the computer does not clearly support this (e.g. at an internet café), Council systems should not be accessed.

11. Monitoring

    As an IT provider, the Council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and employees or councillors are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

12. Reporting security incidents

Any incidents which could pose a risk to the council's systems or data security should be reported to the Clerk without delay. This includes but is not limited to:

(a) lost devices,
(b) potential risk arising from phishing emails/websites,
(c) passwords having been shared, and
(d) unauthorised third-party access to systems.

Where a security breach affects personal data, the Council will follow the ICO guidance and its Data Protection Policy.

13. Training and awareness

The Clerk will advise councillors and staff of relevant training resources and opportunities, including those offered through the county association.

Councillors are strongly encouraged to complete basic cyber security awareness training and report completion of any relevant training to the Clerk.

14. Compliance and consequences

The Council expects its computer systems and email to be used responsibly; inappropriate and unauthorised use will be taken seriously.

Any misuse of Council IT resources by employees may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

Compliance with this policy is part of a councillor's responsibility and breaches may be dealt with under the Member's Code of Conduct.

15. Policy review

This policy was adopted on **27 November 2025**.

This policy will be reviewed every three years to maintain its relevance and effectiveness or when significant guidance changes.