

## Aymestrey Parish Council

### Introduction to IT Security and Email Best Practice for New Councillors and or Staff.

#### 1. Why IT Security Matters

As a councillor, you handle sensitive information about residents, staff, and council business. Protecting this information is not just good practice—it is a legal requirement under the UK GDPR and the Data Protection Act 2018.

A single data breach, phishing attack, or lost password could compromise residents' trust and damage the council's reputation. It is our responsibility to ensure that confidential information is not inadvertently disclosed or accessed by unauthorised individuals.

#### 2. Your Council's IT Setup

The council has one employee (the Clerk/Responsible Officer) and one council laptop, which holds official records and documents.

Councillors currently use personal email addresses for council correspondence. It is therefore especially important to maintain high standards of security, such as regularly updating passwords, using two-factor authentication where available, and ensuring that council-related emails are kept separate from personal ones by using dedicated folders or labels.

Personal devices (phones, tablets, home PCs) may be used to access council information, but councillors are expected to always follow good security practices.

Always lock your device when not in use and avoid sharing it with others. Councillors are required to save parish council documents in a secure folder and to delete sensitive information regularly to minimise the risk of unauthorised access.

#### 3. Risks.

**Think before you click:** Be cautious of emails or links from unknown sources and watch out for phishing attempts that may look legitimate but are designed to steal your information.

**Use strong passwords:** Avoid using easily guessed passwords. Consider using a passphrase or a password manager to keep your credentials secure.

**Update regularly:** Ensure your devices and applications are kept up to date with the latest security patches and updates.

**Report incidents:** If you suspect a security breach or receive a suspicious email, report it to the Clerk/Responsible Officer immediately.

By following these practices, you can help safeguard both council and resident information, maintaining trust and compliance with legal obligations.

[clerk@aymestrey.org](mailto:clerk@aymestrey.org)

14 November 2025.

Drafted by AI and checked by the Clerk/Council.