Elsing Parish Council IT Policy (to be reviewed annually)

Introduction

Elsing Parish Council recognises the importance of secure IT. This policy outlines guidelines for the use of IT resources, and the responsibilities of **A**) Council employees and **B**) Councillors. The former applies to the Clerk, and as required to the auditor and a website technician; the latter to both elected and co-opted members.

Acceptable use of IT resources

NB. Elsing Parish Council has contributed to the cost of the IT resources which its Clerk uses for the business also of other parish councils, who have policies similar to this. It is for the Clerk to alert councils to any apparent contradictions in these policies.

The Clerk's IT resources and Elsing Parish Council's e-mail and web address are to be used only for official council-related activities and tasks. Its users, as in **A**) above, must adhere to ethical standards, respect copyright and intellectual property rights and avoid accessing offensive content. The Clerk is trusted to install only authorised software, and not to use official resources for personal purposes.

Data management

Confidential data should be stored, on computer or on memory sticks, and transmitted securely using approved methods. Regular data backups should be performed to prevent loss, and secure data destruction methods should be used when necessary.

Website

Elsing Parish Council has a dedicated website and its manager is the Clerk. All posts go via the Chair to the Clerk. It is for the Clerk to update, amend or delete posts as appropriate.

Email communication

The Clerk and others occasionally working for her should maintain security of this account, with passwords, which should be strong, changed occasionally and not shared. This applies also to mobile devices. Emails should be retained and archived in accordance with legal and regulatory requirements, or deleted if not needed.

Security incidents

The Clerk is responsible for identifying security breaches, incidents of interference in any IT device by malign third parties, etc, and for taking appropriate action. Such incidents should be reported to Council members.

Councillors

Councillors, as in **B**) above, bear ultimate responsibility for the conduct of all the foregone, whereby complete trust in the Clerk is paramount, and full communication essential. Councillors have their own computers both for personal and Council use, situated in the home where there may be family and visitors. The same degree of security is therefore not possible. Nevertheless, councillors should have regard to the requirements of data protection and GDPR, such as securing by password or encryption information referring to specific individuals or organisations; deleting it when no longer needed; using the bcc function in e-mails, etc.

Adopted: **Date**.....19/1/2026 **Signature**..... **Role**.....Chairman Elsing Parish Council