



EDITH WESTON PARISH COUNCIL INFORMATION TECHNOLOGY POLICY GUIDELINES

Introduction

The purpose of an IT policy is to set out the parameters on how council staff should use the technology that the Parish Council has provided with in order to do their job.

A clear policy will also help to raise awareness of the risks associated with using IT and can protect the council from loss of data.

Staff are not permitted to use IT equipment for personal use (i.e. accessing webmail or online shopping at lunchtimes) nor is it to be used by anyone other than the Parish Clerk. The IT equipment should only be used to carry out official Parish Council business – any other use or abuse will lead to instant dismissal.

Edith Weston Parish Council has the right to monitor work use of IT equipment provided there is a legitimate reason to do so, and that staff have been made aware that this might happen.

The policy applies to the Edith Weston Parish Council Clerk and any other employed staff. It covers computers (laptops), internet access, remote access connections, email servers, file storage, webmail, smart phones, telephones, website, mobile phones etc.

The Chair of Edith Weston Parish Council is responsible for monitoring the implementation of this policy, which has been agreed by Edith Weston Parish Council. This policy should be read in conjunction with all other policies in force within Edith Weston Parish Council.

Guidelines

- Passwords should be kept by the EWPC Clerk and only shared in accordance with the Risk Management Policy/Register. They should not be disclosed to anyone at any time, and should be secure, unique passwords. Any password which becomes known to another person should be changed at the first available opportunity.
- Computer usage – computers should be shut down at the end of every day. The screen should be locked when the employee is away from their desk. Documents should be saved and a regular (monthly) back-up made on a remote hard-drive.
- Personal IT equipment should not be used, with the exception of authorisation codes for secure login when required (e.g. the bank account). EWPC will provide laptop and mobile phone for use.

- Data Protection – the GDPR, Subject Access Request, Freedom of Information and Email policies should be adhered to at all times.
- Mobile phone texting – should be used as a last resort to contact people outside of the Parish Council. Text messages from the council are treated in the same way as emails, for example they must not contain illegal or discriminatory content. Email: the EWPC email policy should be adhered to at all times. Staff should be conscious that they are the public face of the Parish Council and should never use abusive/rude or casual forms of communication nor contain anything that is illegal or discriminatory in content. They should be aware at all times of the risk to the EWPC reputation.
- Internet – the internet can be used for work related issues only – it should not be used for personal use. IT protection is in place through the use of ESET software. Staff should never access sites without a good work related reason.
- Software – software should not be downloaded onto laptops etc unless it has been specifically approved by EWPC.
- Training – can be provided on request and in discussion with the Chair of the Parish Council. The Parish Clerk is expected to have a broad awareness of IT security, GDPR and other issues relating to the use of IT/social media.
- Misuse – misuse of IT facilities can potentially result in disciplinary proceedings. Examples of misuse include not adhering to the policy; attempting to discover a user's password; using the computer systems to act abusively; attempting to circumvent the network's security; knowingly running and installing programmes intended to damage the computer systems; deliberately wasting computer resources; leaving laptops unattended in a public place etc.

This document is based on a template commissioned by the National Association of Local Councils (NALC) for the purpose of its member councils and county associations. Every effort has been made to ensure that the contents of this document are correct at time of publication. NALC cannot accept responsibility for errors, omissions and changes to information subsequent to publication.