

# IT Policy

## 1 Purpose

This policy outlines the acceptable use, management, and security of IT systems and data within Walkern Parish Council. It is designed to:

- Support the council in delivering its duties efficiently and securely.
- Protect personal and council data in compliance with the law.
- Ensure transparency, accountability, and good governance.

## 2 Scope

This policy applies to:

- All councillors, employees, volunteers, and contractors engaged by the council.
- All IT equipment, systems, and services provided or funded by the council.
- Any personal devices used to access or process council information.

## 3 Acceptable Use

- IT systems must be used for official council business only.
- Personal use is permitted only if minimal and does not interfere with council operations.
- Users must not access, store, or distribute offensive, illegal, or inappropriate content.

## 4 Data Protection & Confidentiality

- All personal data must be handled in accordance with the UK GDPR and Data Protection Act 2018.
- Confidential council information must not be shared outside authorised channels.
- Data breaches must be reported immediately to the Clerk or designated Data Protection Office

## 5 Personal Devices (BYOD)

- Personal devices may be used for council business only if adequately protected (passwords, encryption, up-to-date software).
- Council information must be kept separate from personal information where possible.
- Any data loss or breach involving a personal device must be reported immediately.

## 6 Software & Licensing

- Only authorised software may be installed on council devices.

- All software must be properly licensed and regularly updated.
- Users must not download or install software without prior approval.

## **7 Hardware Usage**

- Council-owned devices must be kept secure and used responsibly.
- Any loss, damage, or malfunction must be reported promptly.
- Devices must not be used to access personal social media accounts unless explicitly permitted.

## **8 Internet & Email**

- Council email accounts must be used for all official correspondence.
- Users must avoid clicking suspicious links or opening unknown attachments.
- Internet access must be used responsibly and not for excessive personal browsing.

## **9 Security Measures**

- Strong passwords must be used and changed regularly.
- Multi-factor authentication (MFA) must be enabled where available.
- Devices must be kept updated, secured, and protected with antivirus software.
- Sensitive data must be encrypted when stored or transmitted.

## **10 Remote Working**

- Remote access must be via secure, council-approved methods.
- Devices used remotely must comply with all security protocols.
- Confidential documents must not be printed or stored outside council premises without permission.

## **11 Social Media & Public Communication**

- Only authorised individuals may post on behalf of the council.
- Personal opinions must not be presented as council views.
- All public communication must be respectful and professional.

## **12 Monitoring & Compliance**

- The council reserves the right to monitor IT usage to ensure compliance.
- Breaches of this policy may result in disciplinary action or termination of access.
- Regular audits will be conducted to assess IT security and usage.

## **13 Review**

This policy will be reviewed annually or when significant changes occur in legislation or council operations.

#### **14 Adoption**

This IT Policy was adopted by Walkern Parish Council at its meeting held on 2<sup>nd</sup> October 2025.

#### **15 Review Date**

2<sup>nd</sup> October 2026