



## **Use of IT Policy**

### **Purpose**

The purpose of this policy is to ensure the secure, effective, and lawful use of information technology (IT) systems, devices, and data by employees, councillors, volunteers, and contractors of the Parish Council. It aims to protect the council's IT assets, uphold data protection principles, and promote responsible IT usage.

The Parish Council is committed to ensuring that all IT resources are used responsibly, securely, and effectively. This policy sets out the standards for the use of council-owned IT equipment, software, and internet access by council members, employees, and volunteers.

### **Scope**

This policy applies to all individuals who access or use the Parish Council's IT systems, including:

- Councillors
- Employees
- Volunteers
- Contractors
- Third-party service providers (where applicable)

It covers the use of:

- Council-owned computers, phones, tablets, and other electronic devices
- Email and internet access
- Software, data, and digital services
- Remote and cloud-based systems

### **Acceptable Use**

All users must:

- Use IT equipment and services only for council-related work and in accordance with this policy.
- Keep login credentials secure and not share passwords.
- Use council email addresses for official correspondence.



- Ensure sensitive or confidential data is handled appropriately and securely.
- Report suspected data breaches, malware, or IT issues immediately.

## **Unacceptable Use**

The following are strictly prohibited:

- Using council IT systems for personal gain, illegal activities, or political campaigning.
- Accessing, storing, or sharing offensive, abusive, or inappropriate content.
- Installing unauthorised software or altering system settings.
- Using council devices to conduct private business or unrelated activities.
- Connecting unapproved personal devices to council networks without prior consent.

## **Data Protection and Confidentiality**

All users must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This includes:

- Keeping personal data secure and confidential.
- Not disclosing information without proper authorisation.
- Using encryption and secure storage where required.

## **Email and Internet Use**

- Council email must be used professionally and responsibly.
- Emails sent on behalf of the council must be accurate, respectful, and relevant to council matters.
- Internet usage should be appropriate and in line with council responsibilities.
- Internet access is provided primarily for official duties. Personal browsing must be minimal and not interfere with work responsibilities.
- Users must not download unauthorised software or access inappropriate websites.

## **Security and Updates**

- Users must not disable or bypass antivirus or security settings.
- Council devices must be kept up to date with security patches and software updates.



- Lost or stolen devices must be reported immediately.

## Remote Working

When working remotely:

- Use council-approved devices or ensure personal devices meet security standards.
- Avoid using public Wi-Fi without a secure connection (e.g. VPN).
- Maintain confidentiality, especially in shared or public spaces.

## Monitoring and Compliance

- The council reserves the right to monitor IT usage where legally permitted.
- Breaches of this policy may result in disciplinary action or withdrawal of IT privileges.
- Serious breaches may be reported to the Information Commissioner's Office (ICO) or law enforcement.

## Policy Review

This policy will be reviewed annually or sooner if significant changes occur in technology, legislation, or council operations.

Review Date	Reviewed By	Amendments	Minute Number