

# **UGBOROUGH PARISH COUNCIL IT Policy**

**Adopted by Council September 2025**

**Revised March 2026**

## **Introduction**

Ugborough Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by Council members, employees, volunteers and contractors.

## **Scope**

This policy applies to all individuals who use Ugborough Parish Council's IT resources, including computers, software, devices, data and email accounts.

## **Acceptable use of IT resources and email**

Ugborough Parish Council IT resources and email accounts are to be used for official Council related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy.

All users must adhere to ethical standards, respect copyright and intellectual property rights and avoid accessing inappropriate or offensive content.

## **Device and software usage**

Where possible, authorised devices, software and applications will be provided by Ugborough Parish Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Clerk and Councillors may use their personal devices for council business.

## **Data management and security**

All sensitive and confidential Ugborough Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss and secure data destruction methods should be used when necessary.

## **Email communication**

Email accounts provided by Ugborough Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be attached to emails unless it is encrypted. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking the links.

## **Password and account security**

Ugborough Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

## **Email monitoring**

Ugborough Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

## **Retention and archiving**

Emails should be retained and archived in accordance with legal and regulatory requirements. Users should regularly review and delete unnecessary emails to maintain an organised inbox.

## **Reporting security incidents**

All suspected security breaches or incidents and email related security incidents should be reported immediately to the clerk for investigation and resolution.

## **Training and awareness**

Training and resources are available to inform users about IT security best practices, privacy concerns and technology updates. All employees and councillors should receive regular training on email security and best practices.

## **Compliance and consequences**

Breach of this IT and email policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

## **Contacts**

For IT-related enquiries or assistance, users can contact the Parish Clerk.

All staff and councillors are responsible for the safety and security of Ugborough Parish Council's IT and email systems. By adhering to this IT and email policy, Ugborough Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

## **Review**

Due for review September 2028, or as appropriate.