UGLEY PARISH COUNCIL
Information Technology (IT) Policy

Approved & Adopted by Ugley Parish Council **New Policy**	**Full Parish Council meeting on** **18 May 2026.**

1. Introduction

Ugley Parish Council values secure IT and email use to support its work. This policy sets guidelines for proper use of IT resources and email by council members, staff, volunteers, and contractors.

2. Scope

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

3. Acceptable use of IT resources and email

Ugley Parish Council IT resources and email accounts are for official council work. Some personal use is allowed if it doesn't affect job duties or break this policy. Users must act ethically, respect copyright and intellectual property, and avoid inappropriate content.

4. Device and software usage

Ugley Parish Council will supply approved devices, software, and apps for work. Installing unauthorized or personal software on these devices is strictly forbidden for security reasons.

5. Data management and security

All sensitive and confidential Ugley Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss.

6. Network and internet usage

Ugley Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Ugley Parish Council email accounts are for official use only; keep emails professional. Do not send confidential information unless encrypted. Only open attachments or links from verified sources.

8. Password and account security

Ugley 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.

9. Mobile devices and remote working

Ugley Parish Council mobile devices must be protected using passcodes or biometric security methods. When working remotely, users should maintain office-level security practices.

10. Email monitoring

Ugley 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.

11. Retention and archiving

It is necessary to retain and archive emails according to relevant legal and regulatory requirements. Regularly review your inbox to eliminate unnecessary messages and maintain organisation.

12. Reporting security incidents

All suspected security breaches or incidents should be reported to the Chair and Parish Clerk immediately for investigation and resolution.

13 Training and awareness

Ugley Parish Council will offer regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will be offered regular training on email security and best practices.

14. Compliance and consequences

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

15. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

16. Contacts

For IT-related enquiries or assistance, users can contact the Parish Clerk. All councillors are responsible for the safety and security of Ugley Parish Council's IT and email systems.

By adhering to this IT and Email Policy, Ugley Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.