Stone Parish Council
IT and Email Policy

1. Introduction

Stone Parish Council (hereafter referred to as 'the Council') recognises the importance of effective, secure and responsible use of information technology (IT) and email in supporting the Council's operations, communications and statutory duties.

This policy sets out the responsibilities and expectations for the appropriate use of IT equipment, systems and email by councillors, employees, contractors and volunteers.

2. Scope

This policy applies to anyone using Council IT resources, including computers, laptops, tablets, mobile phones, networks, software, cloud storage, data and email accounts.

Where Council-owned equipment is not available, authorised users may use personal devices for Council business, provided they comply with this policy.

3. Training and Awareness

The Council will encourage users to undertake appropriate cyber security awareness training and keep up to date with current guidance, including resources provided by the National Cyber Security Centre (NCSC), the Parish Council Domain Helper Service and Worcestershire CALC.

4. Acceptable Use of Council IT Resources

Users must use Council IT resources only for legitimate Council business, respect copyright and intellectual property rights, keep Council information secure, not install unauthorised software without the Clerk's approval, and not access or distribute inappropriate or illegal material.

5. Use of Personal Devices

Personal devices used for Council business must be password protected, kept up to date, protected with anti-virus software where appropriate, and Council information kept secure.

6. Internet and Network Security
Only trusted internet connections should be used when accessing Council information. Public Wi-Fi should be avoided unless appropriate security measures are in place.

7. Password and Account Security
Passwords must be strong and unique, stored securely where necessary for business continuity, and multi-factor authentication enabled where available.

8. Email Communications
Council email accounts should be used wherever possible. Emails must be professional, checked before sending, and users should remain alert to phishing emails and suspicious attachments.

9. Email Access
The Council may access Council email accounts where necessary to meet legal obligations or ensure business continuity, in accordance with UK GDPR and the Data Protection Act 2018.

10. Data Management and Security
Council information must be stored securely, backed up where appropriate and retained in accordance with the Council's retention policies.

11. Reporting Security Incidents
Any suspected cyber security incident or data breach must be reported immediately to the Clerk.

12. Compliance
Failure to comply with this policy may result in withdrawal of IT access and disciplinary action where appropriate.

13. Policy Review
This policy will be reviewed every two years or sooner if legislation or technology changes.

14. Contact
Any questions regarding this policy should be directed to the Clerk.

Date adopted:14th July 2026

Review date: May 2027