Old Woughton Parish Council
IT Policy

Reviewed and adopted November 2025

Purpose

This policy sets out how Old Woughton Parish Council (referred henceforth as "the Council"), staff, councillors and authorised users must use Council IT systems and equipment to protect data, ensure security, and support the effective running of Council business.

Scope

This policy covers Microsoft 365 services, accounts created with other third-party service providers for use on behalf of the Council, and access to these systems via any hardware such as laptops, tablets and smartphones, whether they be Council-owned or personal devices.

- The Clerk/RFO
- Councillors
- The Patch Allotment Association (PAA) committee members
- CloudyIT, the Council's contracted managed service provider, who maintain and have access to Council IT systems
- Edge IT Systems Ltd, which provides, maintains, and has access to the Council's allotment management systems

Volunteers and members of the public are not to be provided access to Council IT systems.

Acceptable Use

- Council-owned devices may be used for limited personal use, provided this does not interfere with Council business.
- Councillors must ensure their personal devices are password protected, not shared via family logins, and kept updated with security patches and antivirus software.
- Any Council-related files downloaded to a personal device must be deleted once finished with.
- All users must log out of Microsoft 365 when not in use and never share their login details.

Monitoring

The Council reserves the right to monitor the use of IT systems such as email and file storage where necessary. CloudyIT and Edge IT Systems may also access Council systems as part of their contracted maintenance and support role.

Data Protection

All users must comply with the Council's Data Protection Policy when handling personal data.

Passwords

Strong passwords must be used for all accounts and must not be shared.

Misuse

Misuse of Council IT facilities includes, but is not limited to:

- Using Council accounts or devices for unlawful, abusive or inappropriate activity.
- Attempting to bypass security or access another person's account.
- Installing unauthorised software.
- Failing to keep devices secure.

Breaches of this policy may result in disciplinary action (for staff), removal of access (for councillors or PAA committee members), and/or reporting to relevant authorities.

Responsibility and Review

- All individuals with access to Council IT systems are responsible for reporting immediately any suspected or actual security and/or data breaches to CloudyIT (support@cloudyit.co.uk) or to Edge IT Systems (support@edgeitsystems.com) as appropriate.

- The Clerk is responsible for ensuring compliance with this policy and reporting issues to Council.

- Councillors with IT portfolios will keep abreast of industry best practice and advise the Clerk and Council accordingly.

- CloudyIT and Edge IT Systems will provide technical support and system maintenance in line with their contracted services.

- Due to rapid pace of change in IT, this policy will be reviewed annually.

Review History

November 2025	New policy adopted