

DUDDON PARISH COUNCIL

IT & Data Protection Policy

Adopted on 26th March 2026 – Reviewed 28th May 2026

Purpose:

This policy explains how the Council manages its IT systems and protects personal data. It supports good security practice and meets UK GDPR and Data Protection Act requirements. Scope Applies to all councillors, staff, contractors and volunteers who access Council systems or data.

Roles:

Data Controller: Duddon Parish Council

Data Protection Lead: Parish Clerk

IT Support Provider: TEEK

IT Use:

- Use Council devices for Council work where possible.
- Personal devices must have a password or PIN and be kept updated.
- Only approved software and cloud services may be used.
- Keep devices secure and report loss or damage immediately.

Access & Passwords:

- Each user must have their own account.
- Passwords must be strong and not shared.
- Access is removed when a person leaves their role.

Email & Communication:

- Use Council email accounts for Council business.
- Be careful with links and attachments.
- Check recipients before sending sensitive information.

Data Protection:

- Collect only what is needed.
- Keep data accurate and stored securely.
- Limit access to those who need it.
- Do not keep data longer than necessary.

Data Storage:

- Store data in approved Council systems or secure paper files.
- Avoid USB sticks unless encrypted.
- Do not store Council data in personal accounts unless authorised.

Data Sharing:

- Share personal data only when there is a lawful reason.
- Agreements must be in place when using third-party services.

Data Breaches:

- Report any loss, unauthorised access or mistaken disclosure immediately.
- Serious breaches may be reported to the ICO within 72 hours.

Councillor Responsibilities:

- Keep Council information secure on all devices.
- Delete or return Council data when leaving the Council.

Training & Review:

Basic training will be provided. The policy will be reviewed annually.