STRETTON ON DUNSMORE PARISH COUNCIL

IT Policy

1. PURPOSE

This policy sets out how Stretton on Dunsmore Parish Council manages its information technology systems, data, and digital communications. It applies to all councillors, the clerk, and any staff or volunteers who access council IT systems or handle council data.

This policy supports compliance with SAPPP Assertion 10 (Digital and Data Compliance), the UK General Data Protection Regulation (UK GDPR), and the Data Protection Act 2018.

2. SCOPE

This policy covers:

- Council email and communications
- Council website and domain
- Data storage and backup
- Device use (council-owned and personal)
- Password and access management
- Cybersecurity
- Social media accounts
- Data handover procedures
- Incident response

3. EMAIL AND COMMUNICATIONS

3.1 All council business must be conducted using official council email addresses on the council domain https://stretton-on-dunsmore-parishcouncil.gov.uk/ Personal email accounts (Gmail, Outlook, Yahoo, etc.) must not be used for council correspondence.

3.2 The official council email address is clerk@stretton-on-dunsmore-parishcouncil.gov.uk.

3.3 Council email accounts are council property. When a councillor or officer leaves their role, their access to council email must be revoked and any council correspondence transferred.

3.4 Councillors must not use personal email for forwarding council business. If a councillor receives council-related correspondence on a personal account, they should forward it to the official council email and delete the personal copy.

4. COUNCIL WEBSITE AND DOMAIN

4.1 The council website https://stretton-on-dunsmore-parishcouncil.gov.uk/ must be hosted on a domain registered to the council (not to an individual).

4.2 Domain registration must be in the name of Stretton on Dunsmore Parish Council. The clerk and at least one councillor should have administrative access to the domain registrar account.

4.3 The website must meet WCAG 2.2 AA accessibility standards as required by the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.

4.4 An accessibility statement must be published on the website and reviewed at least annually.

4.5 The council must publish all information required by the Transparency Code for Smaller Authorities, including the publication scheme.

5. DATA STORAGE AND BACKUP

5.1 Council data must be stored in a cloud storage service with UK-based or EU-based data centres.

5.2 The clerk must verify backup integrity at least quarterly by confirming that recent files can be restored.

5.3 Council data must not be stored solely on personal devices, USB drives, or personal cloud accounts.

6. DEVICE USE

6.1 Council-owned devices (laptops, tablets, phones) are for council business only.

6.2 Council devices must have:

- Up-to-date operating system and security patches

- Antivirus/anti-malware software

- Screen lock enabled (maximum 5-minute timeout)

- Full-disk encryption enabled

6.3 Where councillors or staff use personal devices for council business:

- Council data must be accessed via the official email system, no personal information downloaded to the personal device

- The device must have a screen lock and up-to-date software

- If the device is lost or stolen, the owner must notify the clerk immediately

- When the person leaves their council role, all council data must be removed from the device

7. PASSWORD AND ACCESS MANAGEMENT

7.1 All council accounts must use strong passwords (minimum 12 characters, mix of letters, numbers, and symbols).

7.2 Passwords must not be shared between individuals. Each user must have their own login credentials.

7.3 The clerk must maintain a secure record of all council account credentials. This record must be accessible to the council (not just the clerk) in case of emergency.

8. CYBERSECURITY

8.1 All users must be vigilant against phishing emails. Do not click links or open attachments from unknown or suspicious senders.

8.2 Software on council devices must be kept up to date. Security updates should be applied within 14 days of release.

8.3 If a security incident is suspected (phishing, malware, unauthorised access), the clerk must be notified immediately. The clerk will assess the incident and, if personal data is involved, consider whether notification to the ICO is required within 72 hours.

9. SOCIAL MEDIA

9.1 Council social media accounts are council property and must be managed via official council email credentials.

9.2 Only authorised individuals may post on behalf of the council. Posts must be factual and professional.

9.3 Social media must not be used to share personal data or confidential council information.

9.4 Comments and messages received via social media that constitute FOI requests, complaints, or other formal correspondence must be redirected to the official channels.

10. DATA HANDOVER

10.1 When the clerk or any officer with access to council IT systems leaves their role, the following must be transferred to their successor:

- All council email account credentials

- Domain registrar access

- Website administration access

- Cloud storage access

- Social media credentials (if applicable)

- Any encryption keys or password manager access

- Physical devices owned by the council

10.2 The outgoing officer must confirm in writing that they have:

- Transferred all council data
- Deleted council data from personal devices
- Returned all council-owned equipment
- Revoked their own access to council accounts

10.3 The incoming officer must change all shared passwords within 7 days of taking over.