St Mellion Parish Council IT policy:
Initial ideas document originally drafted 25th July 2018
Updated 17the August 2023
Reviewed: February 2024
Adopted: 14th May 2024

INTRODUCTION:

St. Mellion Parish Council stores many forms of data, some of which contain personal information which could be a target for cybercrime such as ransomware, DDOS, etc.

The parish council recognises that it has a legal obligation to secure confidential information.

Communication media need to be managed effectively to ensure data is protected whilst sharing relevant information.

Social media provides a medium where data is readily available, and the parish council has a responsibility to communicate fairly and without bias.

All users need to be aware that personal emails are subject to Freedom of Information Requests/Subject Access Requests if they relate to council business or an individual. It is a criminal offence to block the release of data except where that data is protected under GDPR-UK and the Data Protection Act 2018.

This document provides the policy framework through which data can be managed and communicated. It covers:

- Cyber Security Protocols
- Acceptable Usage
- Social Media

The purpose of this policy is to set out essential protocols to ensure that St. Mellion Parish Council operates to reduce as far as possible the risk of becoming subject to a data breach or any form of cybercrime.

All staff and Councillors are required to read and comply with the conditions of this policy in respect of the way in which the communications mechanisms are used.

The policy includes computers and all other electronic media, the mailbox that the parish council has provided you with and any use by you of your own personal devices.

A. CYBER SECURITY PROTOCOLS

A1. Councillors

i. Email addresses

- Used solely for PC business.
- Used just by the Councillor.
- Accessible only to the Councillor, password to be kept securely and not shared.
- The Parish Clerk has admin rights to set up or delete councillor accounts as required at election, co-option and resignation.

ii. Documents and emails

- The default option is to have all documents in digital format, hard copy only to be used in cases where no other option is available (for example, physical signature required).
- All digital documents to be stored on a secure flash drive, or accessed via secure storage drive, no materials should be stored on PC hard drives or tablets.
- Documents containing no sensitive data can be shared via email but the email and associated download copies to be deleted when no longer required.
- Documents containing sensitive data to only be shared via link to secure storage drive or handed over on an encrypted flash drive, never by email and never downloaded.
- After each PC meeting (also after leaving the role of Councillor), soft copy documents and emails to be deleted from all devices and emptied from all related trash folders.
- Councillors and clerk to delete received/sent emails and email threads when no longer administratively relevant and empty trash folder regularly.

A2. Clerk

- Laptop to have an operational Firewall.
- Clerk has responsibility to ensure that the above cyber security tools are up to date and to request approval for renewal of contracts, upgrades and purchase of new software when costs are incurred.
- Download folder to be expunged and recycle bin emptied at end of each working session.
- Email account is accessible on smart phone and via webmail.
- Emails to be subject to monthly housekeeping as follows: trash folder to be emptied at least weekly; inbox to be weeded monthly, email folders to be weeded every year in August.
- All files to be stored on the work copy USB flash drive, never the hard drive of laptop or PC.
- At end of each working session, flash drive to be ejected and computer shutdown.
- Back-up to encrypted flash drive to be completed weekly using one of two USB drives.

- At monthly meeting the encrypted USB drive is to be kept by the Chair and swapped with the Clerk on a monthly basis.
- Email addresses in the contacts folder to be reviewed annually in August and either 'reconsent' or delete.
- iPhone: delete voicemails after use: delete received and sent text messages monthly; delete received/dialed/missed calls monthly; review stored numbers annually in August and either 'reconsent' or delete private numbers.
- All documents are to be managed as per GDPR guidelines and PC's document retention policy.
- Clerk to use of PC email address for PC business only - no personal use

A3. On-line Accounts & Communications

- Cookies to be deleted from PC or laptop as part of weekly clean up protocol.
- Passwords and logins kept on a spreadsheet on the secure flash drive.
- Two-step authentication to be deployed wherever possible.
- The councillors and clerk have a WhatsApp group to allow urgent contact with each other in the event of national or local emergency or for other issues which require an immediate response, this is set to delete messages after 7 days and is not intended for use for official communication.

A4. PC website

- The current webmaster is Western Web Ltd, Western House, Lamerton, Tavistock, PL19 8QY, 01822 870269, www.westernweb.co,uk
- The website is compliant with WCAG 2.0 Level AA accessibility standards.
- Management of log-in/password details – copy of all email and website passwords to be held by clerk on secure flash drive and by Western Web Ltd.
- Details on the PC website: Cllr title and name; PC postal address (i.e. St Mellion church hall); and PC mobile phone number (no email addresses)
- Enquiries form with Captcha is provided for unsolicited contact.

A5. PC owned IT equipment

- PC owned laptop (current model is HP 250 GN 16gb purchased September 2023)
- Second laptop kept by Clerk, never connected to the internet, data loaded from USB drive at monthly meeting to be shown on projector.
- Projector used at meetings to display agenda, payment schedule, quarterly review and any relevant materials such as reports etc. Never to be used with any materials containing personal data.
- All of the above equipment are Parish Council assets and are included on the insuranace and audit asset schedules.

B. ACCEPTABLE USAGE

The Council recognises that access to professional information by email or through websites is a necessary requirement of the job of Clerk to the Council and other staff and is permitted. Staff and users are expected to use technology in a courteous, reasonable and responsible manner.

The following activities are not acceptable, anyone found to be involved in them may face disciplinary action. In certain instances, the matter will be gross misconduct or a breach of the Code of Conduct.

- Receiving, sending or displaying messages or pictures that are offensive or may be construed to be offensive in nature.
- Using obscene language.
- Improper use of email and internet.
- Damaging computers, computers systems or computer networks.
- Violating copyright laws.
- Using others' passwords and identities.
- Issuing of passwords to third parties unless authorised to do so.
- Trespassing in others' folders, works or files.
- Intentionally wasting limited resources.
- Employing the system for commercial purposes.
- Employing the system for illegal activities.
- Downloading any commercial software.
- Sharing data/information supplied by the Council or residents where consent has not been given.

- Any breaches of GDPR-UK and the Data Protection Act 2018 must be reported immediately to the Information Commissioners Office.

In addition, the following points are to be adhered to:

- The Council encourages electronic communications with local, national and international organisations.
- The Council cannot control and is not responsible for the accuracy or content of information gathered over the internet.
- Security is maintained by appropriate software, internal computer security settings and passwords.
- It is a requirement of the Council and the duty of all staff to avoid deliberate use of the Council's internet connections and technology for inappropriate use. Staff should immediately alert the Clerk to the Council, or the Chair of the Council of any suspect material found stored on any computer.
- The computer equipment and software must be used as installed. Staff and users may not install/uninstall, delete or change anything on Council computers.
- Any requirements to change anything should be authorised by the Clerk to the Council and/or the Chair of the Council.
- The Council uses a virus-checker on the computers. Staff are forbidden to load disks or memory sticks that have not been virus checked by the system.
- Staff or councillors using their own devices must use anti-virus software to maintain security of their system.
- Access to chat rooms, gaming and other associated sites are not permitted on Council computers.
- The Parish Council's email address and IT equipment is only to be used for Parish Council business and must not be used for other personal use.

C. SOCIAL MEDIA

Social media is a generic term for the sharing options, gossip, discussions, stories, video, pictures and information electronically.

The key feature of such systems is that they can be accessed in different ways – via computers, tablets and phones. Examples of popular social media tools include Twitter, Facebook, Wikipedia, YouTube, Pinterest, LinkedIn. Next Door, Instagram et al.

Groupings of interest are a natural feature of the development of such systems with people with similar interests being attracted to share information.

Councillors need to be aware that, when using social media, the Code of Conduct applies to all posts that can be construed as being made in your official capacity. You may wish to consider running a social media account for personal use that is separate from your posts as Councillor.

When staff and Councillors are using social media sites, they should always follow these guidelines:

- Information published on social media should be deemed relevant to the Parish Council or the community that it represents.
- Information should be accurate, fair, thorough and transparent.
- Be aware that what is published will be in the public domain indefinitely.
- Compliance with data protection, intellectual property and copyright laws should be ensured.
- Details about customers, partners, or suppliers should not be referred to without their prior written consent (ensuring no advertisement of the services or goods of third parties).
- Staff and Councillors must refrain from promoting themselves as working for the Council in a way which has, or may have, the effect of bringing the Council into disrepute.
- Staff and Councillors must not disclose personal data or information about the Council or its service users, employees or Councillors that could breach the Data Protection Act 2018 (e.g. photographs, images).
- Staff and Councillors must not make any defamatory remarks about the Council, its service users, employees, Councillors, members of the public or conduct themselves in a way that is detrimental to the Council.