Adopted 13.05.25

Readopted 14.04.26

MARY TAVY PARISH COUNCIL

IT & CYBERSECURITY POLICY

CONTENTS

Introduction....3
General Principles....3
Training and Guidance....3
General IT Policy....4
Employees/Volunteers....4
Members....4
Websites and Social Media....5
Password Protection....5
Portable Devices....6
Incident reporting....6
Misuse of IT....7

INTRODUCTION

1.1 Mary Tavy Parish Council has a duty to ensure the proper security and privacy of its computer systems and data. All users have some responsibility for protecting these assets.

1.2 The Parish Clerk is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.

1.3 Line managers have a responsibility to ensure that staff they supervise comply with this policy

GENERAL PRINCIPLES

1.4 All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in any doubt should seek guidance from the Parish Clerk. As a general rule, users will never be asked to share passwords by email and users should be aware of odd language used in emails which may indicate a fraudulent email.

1.5 All employees, members and other users of council IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection & Retention Policy'.

1.6 All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without the authorisation of the Parish Clerk.

1.7 All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstances may be a criminal offence under the Computer Misuse Act 1990.

1.8 All software installed on council devices must be fully licensed and no software should be installed without authorisation from the Parish Clerk.

TRAINING AND GUIDANCE

1.9 Employees and volunteers will be provided with regular cybersecurity training as is appropriate for their role and level of systems access.

1.10 Members will be provided with a brief overview of cybersecurity measures as part of induction and may be provided with more in-depth training as required.

GENERAL IT POLICY

EMPLOYEES/VOLUNTEERS

2.1 All employees will be assigned a council email address as appropriate. Volunteers may also be assigned a council e-mail address where necessary.

2.2 Personal use of Council IT equipment is permitted but should be kept to a minimum during working hours. Reasonable use of the internet during working hours is permitted.

2.3 The council reserves the right to monitor all activity on company devices. This includes monitoring of clocking in and out, email activity and internet usage for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. Information acquired through such monitoring may be used as evidence in disciplinary proceedings. Monitoring usage will mean processing personal data.

MEMBERS

2.4 All members will be provided with a council e-mail address and must use this for all council business.

2.5 Members are reminded that any e-mail sent or received in their capacity as a Parish Councillor is Council data and any e-mails may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act. This includes e-mails on Personal Accounts when acting as a Councillor.

2.6 A copy of all e-mail received on the councillor e-mail accounts is kept on the server in line with the council's Data Protection and Retention Policy.

2.7 A copy of all e-mail sent from councillor e-mail accounts on the webmail is kept on the server; it is recommended that members not using webmail to access e-mail should set up a rule to ensure a copy of e-mail is kept on the server.

2.8 Members using social media in their capacity as councillors must make it clear they are speaking in a personal capacity and not representing the view of the council.

2.9 Members should ensure they are adhering to the Council's code of conduct when using social media.

2.10 Members must ensure that any personal devices used to access council systems (including email, websites and data) are password protected and access is restricted solely to the member.

WEBSITES AND SOCIAL MEDIA

3.1 Officers shall ensure that any websites operated by the council are regularly reviewed to ensure content is accurate and up-to-date. Websites shall also be monitored for unauthorised access and abuse.

3.2 Council social media accounts will be operated by officers.

3.3 All council social media messages must be non-political, uncontroversial and used to promote/highlight the Parish.

3.4 Approval must be obtained from the Parish Clerk prior to the creation of any council websites or social media accounts.

3.5 All social media messages must be non-political, uncontroversial and used to promote and highlight the Parish.

PASSWORD PROTECTION

7.1 All council computers and systems must be password protected to prevent unauthorised access.

7.2 Where possible, two factor authentication should be utilised.

7.3 Users should ensure that unattended devices are password protected.

7.4 Passwords must confirm to the following criteria:

a. Minimum eight characters
b. Comprise at least one upper case letter, one lowercase letter, one number and one special character

7.5 Where possible, generic user accounts should be avoided.

7.6 Where users have unique access permissions and/or accounts for systems, these must not be shared with other users

7.7 Different passwords should be used for different devices and accounts.

7.8 Passwords should be routinely changed.

7.9 Passwords should not be written down or left in unsecure locations.

PORTABLE DEVICES

5.1 All portable devices (including tablets and mobile phones) must be protected to prevent unauthorised access. This can be by use of passwords, passcodes or other biometric measures as applicable.

5.2 Passcodes must be appropriate for the device and the level of risk that unauthorised access poses to the organisation; where devices can access council data or other systems, passcodes must be unique and not easily guessable.

5.3 Particular care must be taken when using removable media to transmit data as such media are easily lost or intercepted. Any sensitive information (including personal data, confidential documents or data which could impact on the rights or reputation of any person or organisation including the council) placed on removable media must be suitably password protected or encrypted.

INCIDENT REPORTING

6.1 All members, employees or volunteers must report any incidents which could pose a risk to the council's systems or data security to the Parish Clerk without delay. This includes but is not limited to:

a. Lost devices
b. Potential risk arising from phishing emails/websites
c. Passwords having been shared

d. Unauthorised access to systems

MISUSE OF IT

7.1 IT systems will be monitored for misuse and all misuse is prohibited.

7.2 Misuse includes, but is not limited to:

a. Creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material
b. Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
c. Creation or transmission of defamatory material
d. Transmission of material which in anyway infringes the copyright of another person
e. Transmission of unsolicited commercial advertising material to networks belonging to other organisations
f. Deliberate actions or activities with any of the following characteristics:
    i. Wasting staff effort or networked resources
    ii. Corrupting or destroying another users' data
    iii. Violating the privacy of other users
    iv. Disrupting the work of other users
g. Other misuse of the networked resources by the deliberate introduction of viruses/malware
h. Playing games during working hours
i. Altering the set up or operating perimeters of any computer equipment without authority.

7.3 Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited

The IT & Cybersecurity Policy was readopted on 14th April 2026 at Full Council. The next review will be April 2027.