GRAPPENHALL AND THELWALL PARISH COUNCIL
IT and CYBERSECURITY INTERNAL POLICY

(Adopted at the Council Meeting on …….. 2026 V1)

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 Grappenhall and Thelwall 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 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.

1.4 The Council will maintain appropriate technical and organisational measures to protect Council information, systems, devices and data against unauthorised access, loss, destruction, alteration, disclosure, misuse, malware, cyberattack and other security threats.

1.5 The Council will identify, assess and manage information-security and cybersecurity risks as part of its wider risk-management arrangements. Significant risks will be recorded on the Council's risk register and appropriate controls will be implemented and reviewed.

GENERAL PRINCIPLES

1.6 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 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.

1.7 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'.

1.8 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 Clerk.

1.9 Council computers, operating systems, applications and other software must be kept appropriately updated and security patches installed within a reasonable period having regard to the level of risk. Unsupported software or operating systems should not be used for Council business unless specifically authorised by the Clerk and appropriate mitigating controls are in place.

1.10 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.

1.11 All software installed on Council devices must be fully licensed and no software should

be installed without authorisation from the Clerk.

1.12 Council IT equipment and information assets remain the property of the Council, unless otherwise expressly agreed. Users are responsible for taking reasonable care of Council equipment and must report loss, theft, damage or suspected compromise without delay.

1.13 Council equipment, including computers, tablets, mobile telephones, removable media and other devices, must be returned to the Council when no longer required and securely disposed of or recycled in accordance with the Council's data-retention and disposal requirements. Council data must be securely removed before equipment is disposed of, transferred or reused.

TRAINING AND GUIDANCE

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

1.15 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.

1.16 Training will include, where appropriate, phishing and social-engineering awareness, password security, secure use of devices and removable media, reporting of security incidents and the protection of personal and confidential information.

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 Council 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.

2.4 Monitoring will be carried out proportionately and transparently and in accordance with applicable data-protection and employment requirements. Users will be informed about the nature and purposes of monitoring through the Council's relevant privacy and employment documentation.

MEMBERS

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

2.6 Members are reminded that any e-mail sent or received in their capacity as a Councillor is Council data and any e-mails may have to be disclosed following requests under the Freedom of Information Act 2000 or where otherwise required or permitted by applicable data-protection legislation. This includes e-mails on personal accounts when acting as a Councillor.

2.7 A copy of all e-mails received on the Councillor e-mail accounts is kept on the server in line with the Council's Data Protection and Retention Policy.

2.8 A copy of all e-mail sent from Councillor e-mail accounts on the webmail is kept on the server; members should use the Council's approved systems for Council business and must not use personal email accounts where doing so would circumvent the Council's information-security, data-protection or records-management arrangements.

2.9 Members using social media through personal accounts in their capacity as Councillors should make clear when they are expressing a personal view. Official Council social-media accounts must only be used in accordance with the Council's instructions and authorised purposes.

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

2.11 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.

2.12 Access to Council systems will be provided only where required for a legitimate Council purpose and will be limited to the information and functions necessary for the user's role. User access will be reviewed when roles or responsibilities change and will be removed or amended promptly when an employee, volunteer or member leaves the Council or no longer requires access.

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 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.

3.6 Access to Council websites, social-media accounts and associated administrative systems must be restricted to authorised officers. Where practicable, more than one authorised officer should have appropriate administrative access to avoid reliance on a single individual.

PASSWORD PROTECTION

4.1 All Council computers and systems must be password protected to prevent unauthorised access.

4.2 Where possible, two factor authentication should be utilised.

4.3 Users should ensure that unattended devices are password protected.

4.4 Passwords must conform 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

4.5 Where supported by the system, passwords should be at least 12 characters or use a strong passphrase. The Council will follow the security requirements of the relevant system where these provide stronger protection.

4.6 Where possible, generic user accounts should be avoided.

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

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

4.9 Passwords must be changed immediately where they are known or suspected to have been compromised and may otherwise be changed where required by the relevant system or following a security assessment.

4.10 Passwords should not be written down or left in insecure locations.

4.11 Where practicable, multi-factor authentication should be enabled for systems containing personal, confidential or financially sensitive Council information.

4.12 User accounts and access permissions should be reviewed periodically to ensure that access remains appropriate and that unnecessary or inactive accounts are disabled or removed.

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.

5.4 Council data should only be stored on portable devices where there is a legitimate business requirement. Where possible, Council data should be accessed through Council-approved cloud or remote-access systems rather than being permanently stored locally on portable devices.

5.5 Lost or stolen portable devices must be reported to the Clerk immediately so that appropriate action can be taken, including disabling accounts, changing credentials or remotely deleting data where those facilities are available.

BACKUP AND BUSINESS CONTINUITY

5.6 The Council will maintain appropriate backups of important Council information and financial records. Backups should be protected against unauthorised access, accidental deletion, malware and other foreseeable risks.

5.7 Backups should be carried out at an appropriate frequency having regard to the

importance and volume of the information concerned. Where practicable, backups should be maintained separately from the primary system and protected from ransomware or other cyberattacks.

5.8 The Council will maintain appropriate arrangements for restoring access to important systems and data following accidental loss, equipment failure, cyberattack or other significant incident. Backup and restoration arrangements should be tested periodically.

INCIDENT REPORTING AND DATA BREACHES

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 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

e. Loss, accidental disclosure or unauthorised transmission of personal or confidential information

f. Suspected malware, ransomware or virus infection

g. Suspected compromise of a Council account or password

6.2 The Clerk will ensure that reported incidents are assessed promptly and appropriate action is taken to contain, investigate and recover from the incident.

6.3 Where an incident involves personal data, the Council's data-breach procedure will be followed and, where applicable, the incident will be reported to the Information Commissioner's Office or affected individuals within the timescales required by law.

6.4 Users must not attempt to conceal, delete or otherwise interfere with evidence relating to a suspected security incident.

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 parameters of any computer equipment without authority.

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

LEGAL AND REGULATORY COMPLIANCE

8.1 The Council will use its IT systems and process personal and confidential information in accordance with applicable legislation, regulations and recognised good practice.

8.2 This includes, where applicable:

a. UK General Data Protection Regulation (UK GDPR);

b. Data Protection Act 2018;

c. Freedom of Information Act 2000;

d. Computer Misuse Act 1990;

e. Copyright, Designs and Patents Act 1988; and

f. applicable employment, confidentiality, records-management and information-security requirements.

8.3 This policy must be read alongside the Council's Data Protection & Retention Policy, Financial Regulations, Risk Management arrangements, Records Management arrangements and any applicable data-breach or business-continuity procedures.

8.4 The Council will periodically review this policy and associated security arrangements to ensure that they remain appropriate having regard to changes in technology, threats, legislation, guidance and the Council's activities.

ASSET MANAGEMENT AND SECURE DISPOSAL

9.1 The Council will maintain an appropriate record of significant IT assets where necessary for effective management, security, insurance and financial control.

9.2 Users must take reasonable care of Council IT assets and must not permit unauthorised persons to use Council equipment or access Council systems.

9.3 IT assets that are lost, stolen, damaged or suspected of being compromised must be reported to the Clerk without delay.

9.4 Before Council equipment is disposed of, transferred or reused, appropriate steps must be taken to securely erase Council information and personal data or otherwise render it inaccessible.

REVIEW AND ASSURANCE

10.1 The Clerk will periodically review compliance with this policy and report significant issues or risks to the Council as appropriate.

10.2 The Council will review this policy at least annually, or sooner where there are significant changes to legislation, technology, cyber threats, Council systems or working practices.

10.3 The effectiveness of the Council's IT and cybersecurity controls may be considered as part of the Council's risk-management, internal-control and internal-audit arrangements.

10.4 Where weaknesses or significant risks are identified, appropriate remedial action will be taken and monitored to completion.