HARTBURN PARISH COUNCIL

DRAFT IT & CYBERSECURITY POLICY

Approved:

1. INTRODUCTION

1.1 Hartburn 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/RFO is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.

GENERAL PRINCIPLES

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

1.4 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.

1.5 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/RFO.

1.6 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.

1.7 All software installed on council devices must be fully licensed and no software should be installed without the authorisation of the Parish Clerk/RFO.

TRAINING & GUIDANCE

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

GENERAL IT POLICY

2.1 All users will be assigned a council email address as appropriate, and this must be used for all council business.

2.2 Members are reminded that an email sent or received in their capacity as a Parish Councillor is council data and any emails must be disclosed following

requests under the Data Protection Act or Freedom of Information Act. This includes emails on personal accounts when acting as a councillor.

2.3 A copy of all emails received are kept in line with the council's Data Protection and Retention Policy.

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

2.5 Members using social media in their capacity as a councillor must make it clear that they are speaking in a personal capacity, not representing the view of the council.

2.6 Members should ensure they are adhering to the council's Code of Conduct when using social media.

2.7 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 The Parish Clerk/RFO 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 unauthorized access and abuse.

3.2 Council social media accounts will be operated by the Parish Clerk/RFO.

3.3 All 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/RFO prior to the creation of any council website or social media account.

PASSWORD PROTECTION

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

4.2 Where possible, two factor authentication must be used.

4.3 Users should ensure that unattended devices are password protected and locked when not in use or left unattended.

4.4 Passwords must conform to the following criteria:

- Minimum of eight characters
- Comprise at least one upper case letter, one lower case letter, one number and one special character

4.5 Where possible, generic user accounts should be avoided.

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

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

4.8 Passwords must be routinely changed.

4.9 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 or risk that unauthorized access poses to the council; where devices can access personal 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 organization, including the council) placed on removable media must be suitably protected or encrypted.

INCIDENT REPORTING

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

- Lost devices
- Potential risk arising from phishing emails/websites

- Passwords having been shared
- 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:

- 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
- Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety
- Creation or transmission of defamatory material
- Transmission of material which in any way infringes the copyright of another person
- Transmission of unsolicited commercial advertising material to networks belonging to other organisations
- Deliberate actions or activities with any of the following characteristics:
    a. Wasting staff effort or networked resources
    b. Corrupting or destroying other users' data
    c. Violating the privacy of other users
    d. Disrupting the work of other users
- Other misuse of the networked resources by the deliberate introduction of viruses/malware
- Playing games during working hours
- 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.