Owston Ferry Parish Council

IT and Cyber Security Policy

INTRODUCTION

1.1 Owston Ferry 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 Clerk is responsible for the implementation and monitoring of this policy.

GENERAL PRINCIPLES

1.4 All employees, Councillors and other users should be aware of the increasingly sophisticated scams and risks posed to cyber security 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.

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

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 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 Clerk.

GENERAL IT POLICY

EMPLOYEES

2.1 Employees will be assigned a council email address as appropriate.

2.2 Personal use of Council IT equipment is not permitted.

2.3 The council reserves the right to monitor all activity on company devices. This includes 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.

COUNCILLORS

2.4 All Councillors will be provided with a council email address and must use this for all council business.

2.5 Councillors are reminded that any email sent or received in their capacity as a Parish Councillor is Council data and any emails may have to 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.

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

2.7 A copy of all email sent from councillor email accounts is kept on the server.

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

2.10 Councillors must ensure that they use the devices provided by the council and only use these devices to access council systems (including email, websites and data) and are password protected and access is restricted solely to the Councillor.

WEBSITES AND SOCIAL MEDIA

3.1 The Clerk will 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 a nominated Councillor and the Clerk.

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

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

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 for accounts 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 possible, generic user accounts should be avoided.

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

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

4.8 Passwords should 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 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 Councillors or volunteers must report any incidents which could pose a risk to the council's systems or data security to the Clerk without delay.

6.2 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
j. Disclosing or forwarding confidential council information or emails to a member of the public or third party without permission from the Clerk

k. Transmission of any communication that does not conform to the Civility and respect Pledge.

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