CYBER SECURITY POLICY

Adopted 18th June 2024

1. Introduction

The more we rely on technology to collect, store and manage information, the more vulnerable we become too severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise Odiham Parish Council's (OPC) reputation.

OPC's Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

2. Purpose

i) To ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring.
ii) To protect the Council from the risk of financial loss, loss of reputation or libel.
iii) To ensure that the equipment is not used so as to cause harm or damage to any person or organisation.

3. Scope

i) This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.
ii) Confidential data includes, but is not limited to:
Personally Identifiable Information (PII) - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Secret information - Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.
Commercial/operationally sensitive data - information whose loss, misuse, or unauthorised access or modification could adversely affect the commercial or operational security of an organisation
Commercial-in-confidence data - Commercially sensitive information which must be kept confidential between relevant parties for example a supplier's trade secrets that were shared in confidence with a council
Special category personal data - personal data that needs more protection because it is sensitive according to UK General Data Protection Regulation (GDPR) - this includes racial, religious, biometric and health data
Criminal offence data - personal data relating to criminal convictions and offences or related security measures
Personal financial data - an individual's personal credit, charge or debit card information; bank account information; band, credit or financial statements; account or PIN numbers and other information relating to an individual's personal finances.
Payment card data - information used to process credit or debit card transactions
Other sensitive or critical data - any other information whose loss, misuse, or unauthorised access or modification could adversely affect security.
iii) This Policy should be read in conjunction with OPC's Data Protection Policy https://odihamparishcouncil.gov.uk/wp-content/uploads/2023/02/Data-Protection-Policy-July-2023.pdf and Social Media and Electronic Communications Policy https://odihamparishcouncil.gov.uk/wp-content/uploads/2024/04/Social-Media-and-Electronic-Communication-Policy-April-2024.pdf

4. Computer facilities: Use of computer systems

i) Subject to anything to the contrary in this policy the equipment must be used for Council business purposes only.

ii) In order to maintain the confidentiality of information held on or transferred via the Council's equipment, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Council's equipment/network. This will be changed regularly and must be kept secure and not shared with anyone. A full list of account details is held by OPC's appointed IT support.

iii) You are expressly prohibited from using the equipment for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Council or its clients other than in the normal and proper course of carrying out your duties for the Council.

iv) In order to ensure proper use of Council computers, you must adhere to the following practices:

- Anti-virus software must be kept running at all times
- Media storage such as USB drives, CD's or portable hard drives will not be permitted unless they have been provided by the IT supplier or approved by Council
- Obvious passwords such as birthdays and spouse names, etc, must be avoided (the most secure passwords are random combinations of letters and numbers)
- All files must be stored on the network/computer cloud drive which is backed up daily to avoid loss of information
- Always log off the computer/network before leaving your computer for long periods of time or overnight

5. Laptop computers, PC's, tablets and smart phones

i) Laptop computers, PC's, tablets and smart phones belonging to the Council along with related equipment and software are subject to all of the Council's policies and guidelines governing non-portable computers and software.

ii) All laptops, PC's and tablets will be encrypted.

iii) When using such equipment:

- You are responsible for all equipment and software until you return it.
- Equipment must be kept secure at all times.
- You must work within the Councils filing/software environment when carrying out Council business to ensure that all data is backed up and accessible by the Clerk.
- If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the Council's attention
- Upon the request of the Council at any time, for any reason, you will immediately return any equipment and all software to the Council
- If you are using your own laptop or PC to connect with the Council's network or to transfer data between the laptop or PC and any of the Council's computers you must ensure that you have obtained prior consent, comply with instructions and ensure that any data downloaded or uploaded is free from viruses

6. Software

Software piracy could expose both the Council and the user to allegations of intellectual property infringement. The Council is committed to following the terms of all software licences to which the Council is a contracting party. This means, that:

- Software must not be installed onto any of the Council's computers unless this has been approved in advance by OPC's IT support, Clerk or Council. They will be responsible for

establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer facilities.

- Software should not be removed from any computer nor should it be copied or loaded on to any computer without prior consent.

7. Email (internal or external use)

i) All Cllrs & Staff will be issued a Council email account which must always be used when transacting on behalf of the PC.

ii) Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending. confidential information by email this should be sent using password protected attachments.

iii) Do not forward email messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

iv) As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

v) Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

vi) Staff will be required to surrender their email account and all of its contents to the Clerk upon leaving the Council.

8. Personal devices

i) When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. As such, use of personal devices should be kept to an absolute minimum.

ii) OPC advises employees use of personal computer, tablet and cell phone secure to:

- Keep all devices password protected.
- Choose and upgrade antivirus software.
- Do not leave their devices exposed or unattended.
- Install security updates of browsers and systems as soon as updates are available.
- Only log into personal accounts and systems through secure and private networks only.

9. Password Policy

To be advised.

10. Monitoring policy

i) The policy of the Council is that we may monitor your use of the equipment.

ii) The Council may from time to time monitor the equipment. Principal reasons for this are to:

- Detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies.
- Ensure compliance of this policy.

- Ensure compliance by users of the Facilities with all applicable laws (including data protection), regulations and guidelines published and in force from time to time

iii) The Council may adopt at any time a number of methods to monitor use of the Facilities. These may include:
- Recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content.
- Recording and logging the activities by individual users of the Facilities. This may include opening emails and their attachments, monitoring Internet usage including time spent on the internet and websites visited.
- Physical inspections of individual users computers, software and telephone messaging services.

iv) The Council will not (unless required by law):
- Allow third parties to monitor the Facilities (with the exception of OPC's appointed IT support); or
- Disclose information obtained by such monitoring of the Facilities to third parties unless the law permits. The Council may be prohibited by law from notifying employees using the equipment of a disclosure to third parties.

11. General guidance

Never leave any equipment or data (including client files, laptops, computer equipment and mobile phones) unattended on public transport or in an unattended vehicle.

12. Breach of the policy

Compliance with this policy is mandatory and forms part of the terms and conditions of employment of staff. Breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Council's disciplinary process.

Anyone who considers that there has been a breach of this policy in relation to personal information about them held by the Council should raise the matter via the Council's formal grievance procedure.