DOWNHAM MARKET
TOWN COUNCIL

CYBER INFORMATION SECURITY POLICY

DATE OF ADOPTION: 21st November 2023
REVIEW: Three years unless changes in legislation dictate

CYBER INFORMATION SECURITY POLICY

1. INTRODUCTION

This Information Security Policy is a key component of Downham Market Town Council's, (hereinafter referred to as the Council), management framework. It sets the requirements and responsibilities for maintaining the security of information within the Council. This policy may be supported by other policies and by guidance documents to assist putting the Policy into practice day-to-day.

2. AIM AND SCOPE OF THIS POLICY

- The aims of this policy are to set out the rules governing the secure management of the Council's information assets by:

- preserving the **confidentiality, integrity and availability** of the Town Council information.
- ensuring that all members of staff are aware of and fully comply with the relevant **legislation** as described in this and other policies.
- ensuring an approach to security in which all members of staff fully understand their own **responsibilities.**
- creating and maintaining within the organisation a level of **awareness** of the need for information.
- detailing how to **protect** the information assets under the control of the Council.
- This policy applies to all information/data, information systems, networks, applications, locations and staff at the Council or supplied under contract to it.

3. RESPONSIBILITIES

- Ultimate responsibility for information security rests with the Town Clerk of the Council, but on a day-to-day basis the Deputy Town Clerk shall be responsible for managing and implementing the Policy and related procedures.

- Responsibility for maintaining this Policy, the Council Information Audit Report and for recommending appropriate risk management measures is held by the Town Clerk. Both the Policy and the the Information Audit report shall be reviewed by the Town Clerk with the Governance Committee annually.

- The Town Clerk is responsible for ensuring permanent staff, temporary staff and contractors are aware of:-
  > The Information security policies applicable in their work areas
  > Their personal responsibilities for information security
  > How to access advice on information security matters

- All staff shall comply with the Information Security Policy and must understand their responsibilities to protect the Council's data. Failure to do so may result in disciplinary action.

- The Town Clerk and Deputy Town Clerk shall be individually responsible for the security of the information systems they use.

- Each member of staff shall be responsible for the operational security of the information systems they use.

- Each system user shall comply with the security requirements that are currently in force, and shall also ensure that confidentiality, integrity and availability of the information they use is maintained to the highest standard.

- Access to the Council's information systems by external parties shall only be allowed where a contract that requires compliance with this Information Security Policy is in place. Such a contract shall require that the staff or sub-contractors of the external organisation comply with all security policies.

4. LEGISLATION

- The Council is required to abide by certain UK, European Union and International legislation. It may also be required to comply to certain Government rules and regulations.

- The requirement to comply with legislation shall be devolved to employees and agents of the Council, who may be held personally accountable for any breaches of information security for which they are responsible.

- In particular, the Council is required to comply with:

- The Data Protection Act (2018)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

5. PERSONNEL SECURITY

Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
- References for new staff shall be verified and a passport, driving licence or other document shall be provided to confirm identity.
- Information security expectations of staff shall be included within appropriate job definitions.
- Whenever a staff member leaves the Council, their accounts will be disabled the same day they leave.

Information Security Awareness

. An on-going awareness programme shall be established and maintained in order to ensure that staff awareness of information security is maintained and updated as necessary.

Intellectual Property Rights

. The Council shall ensure that all software is properly licensed and approved. Individual and Council intellectual property rights shall be protected at all times.
. Users breaching this requirement may be subject to disciplinary action.

6. ACCESS MANAGEMENT

Physical Access

. Only authorised personnel who have a valid and approved Council need, shall be given access to areas containing information systems or stored data.
. **All passwords shall be eight characters or longer and contain at least two of the following: uppercase letters, lowercase letters and numbers.**
. All administrator-level **passwords** shall be **changed at least every 120 days.**
  . Where available, two-factor authentication shall be used to provide additional security.
  . All users shall use uniquely named user accounts.
  . Generic user accounts that are used by more than one person or service shall **NOT** be used.

User Access

. Access to information shall be based on the principle of "least privilege" (a user should only have access to what they absolutely need in order to perform their responsibilities, and no more).

Administrator-level Access

. Administrator-level access shall only be provided to individuals with a Council need who have been authorised by the Town Clerk.
. A list of individuals with administrator-level access shall be held by the Town Clerk and shall be reviewed every 12 months.
. Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

Application Access

. Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate Council need e.g. systems or database administrators.

Hardware Access

. Where indicated by a Risk Assessment, access to the network shall be restricted to authorised devices only.

System Perimeter Access (firewalls)

. The boundary between the Council’s systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.

. All servers, computers, laptops, mobile phones and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device’s operating system.

. The default password on all firewalls shall be changed to a new password that complies to the password requirements in this Policy, and shall be changed regularly.

. All firewalls shall be configured to block all incoming connections.

. If a port is required to be opened for a valid Council reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a Council reason for it to remain open.

Monitoring System Access and Use

. An audit trail of system access and data used by staff shall be maintained wherever practical and reviewed on a regular basis.

. The Council reserves the right to monitor systems or communication activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

7. ASSET MANAGEMENT

Asset Ownership

. Each information asset (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

Asset Records and Management

. An accurate record of Council information assets, including source, ownership, modification and disposal shall be maintained.

. All data shall be securely wiped from all hardware before disposal.

Asset Handling

. The Council shall identify particularly valuable or sensitive information assets through the use of data identification.

. All staff are responsible for handling information assets in accordance with this security policy. Where possible, the data classification shall be marked upon the asset itself.

. All Council information shall be categorised into one of the three categories in the table below based on the description and examples provided.

Category	Description	Example
Public	Information which is not confidential and can be made available publicly any channels.	. Details of products and services on the website . Published Council information . Social media updates . Press releases
Amber Information	Information which, if lost or if made available to unauthorised persons could impact the Council's effectiveness, benefit competitors or cause embarrassment to the Council and/or its partners.	. Council operating procedures and policy . Client contact details . Council plans and financial information . Basic employee information including personal data
Red Information	Information which, if lost or made available to unauthorised persons, could cause severe impact on the Council's ability to operate or cause significant reputational damage and distress to the Council's and/or its partners. This information requires the highest levels of protection of confidentiality, integrity and availability.	. Client intellectual property . Data in e-commerce systems . Employee salary details . Any information defined as "sensitive personal data" under the Data Protection Act

Removable Media

- Only Council provided removable media (such as a USB memory stick and recordable CDs/DVDs) shall be used to store Council data and its use shall be recorded (e.g. serial number, date issued to and returned).
- Removable media of all types that contain software or data from external sources, or that has been used on external equipment, requires the approval of the Town Clerk before they may be used on Council systems. Such media must be scanned by anti-virus software before being used.
- Where indicated by the risk assessment, systems shall be prevented from using removable data.

Users breaching these requirements may be subject to disciplinary action.

Mobile Working

- Where necessary, staff may use Council supplied mobile devices such as phones, tablets and laptops to meet their job role requirements.
- Use of mobile devices for Council purposes (whether Council owned or personal

devices) requires the approval of the Town Clerk.

- Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured, must be encrypted (if available for the device) and be capable of being remotely wiped. They must also comply with the software management requirements within this policy.
- Users must inform the Town Clerk immediately if the device is lost or stolen and Council information must then be remotely wiped from the device.

Personal Devices/Bring Your Own Device (BYOD)

- Where necessary, staff may use personal mobile phones to access Council email. This usage must be authorised by the Town Clerk. The device must be registered in the asset records and must be configured to comply with the mobile working section and other relevant sections of this policy.
- No other personal devices are to be used to access Council information.

Social Media

- Social Media may only be used for Council purposes by using office Council social media accounts with authorisation from the Town Clerk/Deputy Town Clerk. Users of Council social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.
- Council social media accounts shall be protected by strong passwords in-line with the password requirements for administrator accounts.
- Users shall behave responsibly while using any social media whether for the Council or personal use, bearing in mind that they directly or indirectly represent the Council. If in doubt, consult the Town Clerk/Deputy Town Clerk.
- **Users breaching this requirement may be subject to disciplinary action.**

8. PHYSICAL AND ENVIRONMENT MANAGEMENT

- In order to minimise loss of, or damage to, all assets and equipment shall be physically protected from threats and environmental hazards.
- Systems shall be protected from power loss by uninterruptible power supply (UPS, surge protection) if required.
- Systems requiring particular environmental operating conditions shall be maintained within optimum requirements.

9. COMPUTER AND NETWORK MANAGEMENT

Operations Management

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Town Clerk.

System Change Control

- Changes to information systems, applications or networks shall be reviewed and approved by the Town Clerk.

Accreditation

. The Council shall ensure that all new and modified information systems, applications and networks include security provisions.

Software Management

. All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.
. All software security/patches shall be installed within 14 days of their release.
. Only software which has a valid Council reason for its use shall be installed on devices used for Council purposes.
. Users shall not install software or other active code on the devices containing Council information without permission from the Town Clerk.
. For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for Council purposes.

External Cloud Services

. Where data storage, applications or other services are provided by a ‘cloud provider’ there must be confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from Malicious Software

. The Council shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
. All computers, servers, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device’s operating system.
. All anti-malware software shall be set to:
> scan files and data on the device on a daily basis
> scan files on-access
> automatically check for, and install, virus definitions and updates to the software itself on a daily basis
> block access to malicious websites

Vulnerability Scanning

. The Council shall have a yearly vulnerability scan of all external IP addresses carried out by the IT provided.
. The Council shall act on the recommendations of the IT provider following the vulnerability scan in order to reduce the security risk presented by any signifiant vulnerabilities.
. The results of the scan and any changes made shall be reflected in the Council’s Security Policy as appropriate.

10. STAFF AND COUNCILLOR RESPONSIBILITIES

. Staff and Councillors are not to divulge their user credentials to anyone, including family members, unless with the strict approval of the Town Clerk.

. Staff and Councillors are not to leave unlocked devices unattended and all mobile devices should be pin protected. Any stolen device, containing information relating to the Council, must immediately be reported to the Town Clerk.

. Staff and Councillors should be mindful of the risks involved with cybersecurity and should not share any private data or information to a third party. Staff should be satisfied that any websites visiting while browsing the internet on Council devices are legal and safe to use.

. The Town Clerk will routinely remind staff about leaving their computers unlocked and will share on cybersecurity awareness information as appropriate to keep abreast of the latest advice and guidance.

11. RESPONSE

Information Security Incidents

. All breaches of this policy and other information security incidents shall be reported to the Town Clerk and Governance Committee.

. If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Town Clerk.

. Information security incidents shall be recorded and investigated by the Town Clerk to establish their cause and impact with a view to avoiding similar events.

Town Council Continuity and Disaster Recovery Plan

. The Town Clerk shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Further Information

. Further information and guidance regarding this policy can be obtained from the Town Clerk.

12. MONITORING

. This policy will be monitored periodically by the Council to judge its effectiveness and will be updated in accordance to changes in the law. This is a non-contractural procedure which will be reviewed every three years.

END