DUNSTABLE TOWN COUNCIL

INFORMATION SECURITY POLICY

1. Introduction

This information security policy is a key component of the Dunstable Town Council management framework. It sets the requirements and responsibilities for maintaining the security of information within Dunstable Town Council. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day. It is communicated to all staff and contractors to Dunstable Town Council.

2. Aim and Scope of this policy

The aims of this policy are to set out the rules governing the secure management of our information assets by:

- preserving the **confidentiality, integrity and availability** of our business 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 our control

This policy applies to all information/data, information systems, Operational* networks, applications, locations and staff of Dunstable Town Council or supplied under contract to it.

See Section 9, Computer and Network management, for description of the Operational and Test networks.

3. Responsibilities

- Ultimate responsibility for information security rests with the Town Clerk & Chief Executive of Dunstable Town Council, but on a day-to-day basis the Corporate Performance & Compliance Manager shall be responsible for managing and implementing the policy and related procedures.
- Responsibility for maintaining this Policy, the business Information Risk Register and for recommending appropriate risk management measures is held by Dunstable Town Council. Both the Policy and the Risk Register shall be reviewed by the Corporate Performance & Compliance Manager at least annually.
- Managers are responsible for ensuring that their 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 company's data. Failure to do so may result in disciplinary action.
- Line managers shall be individually responsible for the security of information within their business area.
- 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 the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- Access to the organisation'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 contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

4. Legislation

Dunstable Town Council is required abide by certain UK, European Union and international legislation. It also may be required to comply to certain industry rules and regulations.

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

5. Cyber Essentials

Dunstable Town Council uses CyberSmart to obtain and maintain our annual Cyber Essentials certification. It is important to maintain compliance with the Cyber Essentials standard that the controls described throughout this Policy are implemented and reviewed on a regular basis.

6. 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 license 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 company their accounts will be disabled the same day they leave.

Information Security Awareness and Training

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.

- Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff
- An on-going awareness programme shall be established and maintained to ensure that staff awareness of information security is maintained and updated as necessary.

Intellectual Property Rights

- The organisation shall ensure that all software is properly licensed and approved by the Compliance Manager. Individual and Dunstable Town Council intellectual property rights shall be protected at all times.
- Users breaching this requirement may be subject to disciplinary action.

7. Access Management

Physical Access

Only authorised personnel who have a valid and approved business need shall be given access to areas containing information systems or stored data.

Identity and passwords

- Passwords must offer an adequate level of security to protect systems and data
- Passwords shall be changed in the event of a security breach
- All passwords shall be complex, 12 characters long and assigned using a Password Manager.
- All administrator-level passwords shall have
  - Where available, two-factor authentication shall be used to provide additional security
  - All users shall use uniquely named user accounts
  - For services that provide access to business information, generic user accounts that are used by more than one person or service shall not be used.

User Access

- New User Accounts will only be provided with the authorisation of the authorized decision makers as pre agreed with IT Provider.
- Access to information shall be based on the principle of “least privilege” and restricted to authorised users who have a business need to access the information.
- User accounts no longer required will be removed within 24 hours.

Administrator-level access

- Administrator-level access shall only be provided to individuals with a business need who have been authorised by the Compliance Manager.
- A list of individuals with administrator-level access shall be held by the Compliance Manager and shall be reviewed regularly and at least every 6 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 business need e.g. systems or database administrators.
- Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

- Access to the Operational network shall be restricted to devices authorised by the Compliance Manager.

System Perimeter access (firewalls)

- The boundary between business 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 in the event of a security breach.
- All firewalls shall be configured to block all incoming connections.
- If a port is required to be opened for a valid business reason, the change shall be authorised by the Compliance Manager. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
- The business reserves the right to monitor and systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

8. Asset Management

Asset Records and Management

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

Asset Handling

- Dunstable Town Council shall identify particularly valuable or sensitive information assets through the use of data classification.
- All staff are responsible for handling information assets in accordance with this security policy.
- All company information shall be categorised into one of the four 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 through any channels.	• Details of products and services on the website • Published company information • Social media updates • Press releases
Company Confidential	Company related information restricted to employees of the company and not be disclosed to third parties without authorisation	• Company operating procedures and policy • Company plans and financial information • Employee contact information
Company Sensitive	Information which, if lost or made available to unauthorised persons, could cause severe impact on the company's ability to operate or cause significant reputational damage and distress to the organisation and/or its partners. May include personal data.	• Employee salary details • Employee Personal details • Commercial finance arrangements • Contracts
Client Confidential	All technical information pertaining to clients. Access restricted to company employees and subcontractors. May include Personal Data.	• Client intellectual property • Contact details • Systems access information • Technical diagrams, specifications • Project related documents

Removable media

- Only company provided removable media (such as USB memory sticks and recordable CDs/DVDs) shall be used to store business data and its use shall be recorded (e.g. serial number, date, issued to, returned).
- Removable media of all types that contain software or data from external sources or the Test network, that has been used on external equipment, require the approval of the Compliance Manager before they may be used on business systems. Such media must be scanned by anti-virus before being used. Users breaching these requirements may be subject to disciplinary action

Mobile working

- Use of mobile devices for business purposes (whether business-owned or personal devices) requires the approval of the Compliance Manager.

- Such devices 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 Compliance Manager immediately if the device is lost or stolen and business 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 business email. This usage must be authorised by the Compliance Manager. The device 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 business information

Social Media

- Business 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 business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult the Compliance Manager.
- Users breaching this requirement may be subject to disciplinary action.

9. Computer and Network Management

Network Management

Dunstable Town Council manages several networks across various sites as below:

- Grove House HQ: Grove House (Operational Network) and Grove House Public (Public WiFi on separate VLAN)
- Dunstable Bennetts Splash Park: Splash Park (Operational Network) and Splash Park Guest (Public WiFi on separate VLAN)
- Dunstable Cemetery: DTC Cemetery (Operational Network)
- Dunstable Grove Youth Centre: DTC-Grove-Corner (Operational Network) and DTC-Grove-Corner-Guest (Public Wifi on Separate VLAN)
- Dunstable Priory Centre: Priory House (Operational Network)

Public and Guest networks are separated from the operational networks with a VLAN to ensure no access to council data Systems**.**

System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the authorised decision makers. The appointed IT provider will then carried out these changes.

Accreditation

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

- They must be correctly sized, identify the security requirements, be compatible with existing systems according to an established systems architecture (as required) and be approved by the Compliance Manager before they commence operation.

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 updates/patches shall be installed within 7 days of their release.
- Only software which has a valid business reason for its use shall be installed on devices used for business purposes
- Users shall not install software or other active code on the devices containing business information without permission from the Compliance Manager.
- For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for business purposes.

Local Data Storage

- Data stored on the business premises shall be backed up regularly and restores tested at appropriate intervals (at least quarterly).
- A backup copy shall be held in a different physical location to the business premises
- Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

External Cloud Services

Where data storage, applications or other services are provided by another business (e.g. a 'cloud provider') Dunstable Town Council will ensure 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. Common certification standards may include:

- Cyber Essentials
- Cyber Essentials Plus
- ISO 27001

Protection from Malicious Software

- The business 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

10. Response

Information security incidents

All breaches of this policy and all other information security incidents shall be reported to the Compliance Manager.

If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by the Compliance Manager
Information security incidents shall be recorded in the Security Incident Log and investigated by CloudyIT as the IT Provider in conjunction with the Compliance Manager to establish their cause and impact with a view to avoiding similar events. The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.

Reporting

The appointer IT provider to the council will update the Compliance Manager on the security status who in turn shall inform the organisation by means of regular reports to senior management.

Further Information

Further information and guidance on this policy can be obtained from the Corporate Performance & Compliance Manager. Comments and suggestions to improve security are always welcome.