MAESTEG TOWN COUNCIL

Information Security Policy

Introduction

Maesteg Town Council holds data on its employees as well as its members and service users and it is vital that this information is held in accordance with the requirements of the Data Protection legislation. This policy applies to all staff and Councillors depending on the extent of the information they receive from the Town Council.

1. Objectives, Aim and Scope

1.1. Objectives

The objectives of the policy are as follows:-

1.1.1. **Confidentiality** - Access to Data must be confined to those with specific authority to view the data.
1.1.2. **Integrity** – Information is to be complete and accurate. All systems, assets and networks must operate correctly, according to specification.
1.1.3. **Availability** - Information must be available and delivered to the right person, at the time when it is needed.

1.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Town Council by:

1.2.1. Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
1.2.2. Describing the principles of security and explaining how they will be implemented in the organisation.
1.2.3. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
1.2.4. Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
1.2.5. Protecting information assets under the control of the organisation.

1.3. Scope

This policy applies to all information, information systems, networks, applications, locations and users.

2. Responsibilities for Security

2.1. Ultimate responsibility for security rests with the Town Council, but on a day-to-day basis the Town Clerk/RFO will be responsible for managing and implementing the policy and related procedures.

2.2. The Town Clerk/RFO and his/her staff are responsible for ensuring that :-

2.2.1. The information security policies are operated in their work areas

2.2.2. Their personal responsibilities for information security are complied with

2.2.3. They know how to access advice on information security matters.

2.3. All staff must comply with security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

2.4. The Information Security Policy shall be maintained, reviewed and updated by the Town Council and this review shall take place every three years.

2.5. Staff shall be individually responsible for the security of their physical environments.

2.6. Each user shall be responsible for the operational security of the information systems they use.

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

2.8. Contracts with external contractors that allow access to the organisation's information systems will be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

3. Legislation

3.1. The Town Council is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents, who may be held personally accountable for any breaches of security for which they may be held responsible. The Town Council will comply with the following legislation and other legislation as appropriate:

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

4. Policy Framework

4.1. Management of Security

4.1.1. At the Town Council level, responsibility for Information Security will reside with the HR Committee.

4.1.2. The Town Clerk/RFO will be responsible for implementing, monitoring, documenting and communicating security requirements for the Town Council.

4.2. Information Security Awareness Training

4.2.1. Information security awareness training will be included in the staff induction process.
4.2.2. An on-going awareness programme will be established in order to ensure that staff awareness is refreshed and updated as necessary.

4.3. Contracts of Employment

4.3.1. Security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause.
4.3.2. Security Requirements will be included in job definitions.

4.4. Security Control of Assets

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

4.5. Access Controls

Only authorised personnel who have a business need will be given access to restricted areas containing information systems.

4.6. User Access Controls

Access to information will be restricted to authorised users who have a business need to access the information.

4.7. Computer Access Control

Access to computer facilities will be restricted to authorised users who have a business need to use the facilities.

4.8. Application Access Control

Access to data, system utilities and program source libraries will be controlled and restricted to authorised users who have a business need to use the applications. Authorisation to use an application will depend on the availability of a licence from the supplier.

4.9. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment will be physically protected from security threats and environmental hazards.

4.10. Computer and Network Procedures

Management of computers and networks will be controlled by standard procedures that have been authorised by the Town Clerk/RFO.

4.11. Security Incidents and weaknesses

All security incidents and weaknesses are to be reported to the Town Council. All security incidents will be investigated to establish their cause, operational impact, and business outcome.

4.12. Protection from Malicious Software

The organisation will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff will be expected to co-operate fully with this policy. Users must not install software

on the organisation's property without permission from the Town Clerk/RFO. Users breaching this requirement may be subject to disciplinary action.

4.13. User Disks

Disks/memory sticks containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on the Town Council's equipment. Furthermore, the confidentiality and security of information contained in such storage devices must be properly maintained. Employees breaching this requirement may be subject to disciplinary action.

4.14. Monitoring System Access and Use

An audit trail of system access and use will be maintained and reviewed on a regular basis.

4.15. Accreditation of Information Systems

The organisation will ensure that all new information systems, applications and networks include a security plan and are approved by the HR Committee before they commence operation.

4.16. System Change Control

Changes to information systems, applications or networks must be reviewed and approved by the HR Committee.

4.17. Intellectual Property Rights

The Town Clerk/RFO will ensure that all information products are properly licensed and approved by the Town Council. Users must not install software on the Town Council's property without permission from the Town Clerk/RFO. Users breaching this requirement may be subject to disciplinary action.

4.18. Business Continuity and Disaster Recovery Plans

The Town Council will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks.

4.19. Reporting

The Town Clerk/RFO will keep the HR Committee informed of the information security status of the Town Council by means of regular reports.

Adopted by Maesteg Town Council: 01.02.2022

Review Date: (Annually at February Full Council)