Information Security Policy

March 2018

1. Introduction

Information processing as a fundamental part of the Council's business, so it is important that we have a clear and relevant Information Security Policy, to ensure this information is protected against accidental or intentional loss, or unauthorised access, alteration or disclosure.

This policy aims to ensure the following:

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

This policy will achieve these aims through the following key areas:

- **Awareness** - Ensuring that everyone is aware of and fully complies with the relevant legislation as described in this and other policies, and maintaining an organisational level of awareness of the need for Information Security as an integral part of day to day business.
- **Principles** - Describing the principles of security and explaining how they shall be implemented in the Council.
- **Consistency** - Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- **Protection** - Protecting information assets under the control of the Council.

2. Responsibilities

Ultimate responsibility for information security rests with the Parish Council, but on a day-to-day basis the Clerk to the Council and/or the Data Protection Officer (DPO) shall be responsible for managing and implementing the policy and related procedures.

The Council is responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The application of this information security policy to their work areas.
- Their personal responsibilities for information security.
- How to access advice on information security matters.

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity.

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

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.

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

3. Policy Framework

3.1. Management of Security

Overall responsibility for Information Security shall reside with the Parish Council.

The Clerk to the Council and/or the DPO shall be responsible for implementing, monitoring, documenting and communicating security requirements for the Council.

3.2. Information Security Awareness Training

Information security awareness training shall be included in the staff induction process.

An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

3.3. Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions.

3.4. Security Control of Assets

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

3.5. Access Controls

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

3.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

3.7. Computer Access Control

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

3.8. Application Access Control

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 the availability of a licence from the supplier.

3.9. Equipment Security

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

3.10. Computer and Network Procedures

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

3.11. Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence. Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the Council's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

3.12. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Data Protection Officer. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

3.13. Protection from Malicious Software

The Council uses software counter-measures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the Council's property without permission from the Town Clerk. Users breaching this requirement may be subject to disciplinary action.

3.14. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Clerk to the Council before they may be used on the Council's systems. Such media must also be fully virus checked before being used on the Council's equipment. Users breaching this requirement may be subject to disciplinary action.

3.15. Monitoring System Access and Use

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

The Council has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts.
- Investigating or detecting unauthorised use of the system.
- Preventing or detecting crime.
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training).
- In the interests of national security.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures.
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

3.16. Accreditation of Information Systems

The Council shall ensure that all new information systems, applications and networks include a security plan and privacy impact assessment and are approved by the Clerk to the Council and/or the Data Protection Officer before they commence operation.

3.17. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Data Protection Officer.

3.18. Intellectual Property Rights

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

3.19. Business Continuity and Disaster Recovery Plans

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

3.20. Policy Review

This policy will be reviewed at least annually by the Parish Council, the Clerk to the Council and/or the Data Protection Officer.