Information Governance Policy

February 2018

1. Introduction

Information is a vital asset to the Council and may be of value to others and misused in the wrong hands. It is therefore of paramount importance that information is managed efficiently and securely.

2. Purpose

The purpose of this policy is to ensure that information is processed lawfully, fairly, securely and effectively. It supports the council's legal obligations by ensuring compliance with information legislation including the Freedom of Information Act, Data Protection Act and the General Data Protection Regulation.

3. Scope

- This policy applies to the following:
- Information owned by the Council, including information held on the Council's behalf by contractors or partner organisations.
- Information owned by other organisations but accessed by the Council, where no specific information sharing protocol is in place.
- Information in any format or sent or received by any means of transmission e.g. paper, digital photos, scans, emails, databases etc.).
- All employees of the Council, Council members, temporary workers, volunteers etc.
- Employees of any other organisation having access to the Council's information e.g. auditors, contractors and partner agencies, where no specific information sharing protocol is in place.

4. Supporting Policies

This policy is supported by the Council's Data Protection, Freedom of Information and Records Management policies.

5. Principles and Approach

The Council understands the need for an appropriate balance between openness and confidentiality in the management and use of information, and to share information in a controlled manner. It is important to ensure high standards of data protection and confidentiality to safeguard personal data and commercially sensitive information. Underpinning this is the need to ensure that information is accurate, relevant and available only to those who need it. The Council will therefore endeavour to ensure that information is:

- Held securely and confidentially.
- Obtained fairly and lawfully.
- Recorded accurately and reliably.

- Used effectively and ethically.
- Shared and disclosed appropriately and lawfully.
- Held no longer than required.
- Disposed of appropriately.

To protect information from internal, external, accidental or deliberate threats e.g. loss, destruction or theft, the Council will ensure:

- Information is protected from unauthorised access.
- Confidentiality is upheld.
- Integrity of information is maintained.
- Adherence to legislation and regulation.
- A business continuity plan is in place.
- Suitable staff training.
- All breaches, near-misses or potential issues are reported to the Clerk to the Council and/or the Data Protection Officer.

6. Themes

6.1. Openness

None confidential information held by the council will be made available to the public through the council's website.

6.2. Legal Compliance

The Council will ensure its policies comply with the requirements prescribed in relevant legislation including the Data Protection Act, Freedom of Information Act and the General Data Protection Regulation. Council will also respect any intellectual property rights associated with information it uses.

6.3. Information Security

In partnership with the Council's IT services provider, the Council will maintain procedures to ensure the confidentiality and integrity of information and to control its availability.

6.4. Information and Records Management

The Council has a records management policy which sets out standards for handling information during each phase of the lifecycle from collection/creation to final outcome.

6.5. Quality Assurance

The Council will undertake annual assessments and audits of its information quality and records management arrangements.

6.6. Partnerships and Information Sharing

Any sharing of personal information with partner agencies will be subject to an information sharing protocol, which sets out the expected process, security standards and information handling procedures.

7. Key Information Governance Personnel

Day to day responsibility for providing guidance to staff will be undertaken by the Information Risk Owner/Date Protection Officer. The senior management team are responsible for ensuring that sufficient resources are provided to support the effective implementation of information governance in order to ensure legal and statutory compliance.

7.1. Information Asset Owners

This is the Clerk to the Parish Council. The Clerk's duties include:

- Knowing what information comprises or is associated with the asset and understanding the nature of information flows.
- Knows who has access to the asset and why, and monitoring this to ensure compliance.
- Understanding and addressing risks to the asset and providing assurance to the Information Risk Owner.
- Ensuring there is a legal basis for processing data and for any disclosures.
- Refer any queries about the above to the Information Risk Owner.

7.2. Information Risk Owner/Council & Clerk to the Council

The Parish Council (Corporate Body) and the Clerk to the Parish Council's role is detailed in the Data Protection Policy. The key responsibilities of the Information Risk Owner are:

- Developing and implementing information governance procedures processes.
- Raising awareness and providing advice and guidance about information governance.
- Overseeing relevant training.
- Co-ordinating activities relating to data protection, confidentiality, freedom of information, records management and information quality.
- Monitoring compliance with legal and statutory obligations, guidance and procedures.

7.3. Information & Computer Technology Services Provider

The Council must ensure the following:

- Robust ICT security arrangements in line with industry best practice.
- Effective management and security of the Council's ICT resources.
- A robust IT disaster recovery plan.

7.4. The Council

The Council is responsible for implementing the Information Governance Policy within the Council and will ensure the following:

- The requirements of the Information Governance Policy and its supporting policies and guidance are built into local procedures.

- Compliance within their area of responsibility.
- Information governance issues are identified and resolved whenever a service or procedure is changed or created.
- Staff are supported to meet information governance requirements.

7.5. All Staff

Each employee is responsible for adhering to this policy and will receive guidance from the following sources:

- Policies and procedures.
- Line manager.
- Training.
- Team meetings.
- Bulletin emails.