SPENNYMOOR TOWN COUNCIL

INFORMATION RISK MANAGEMENT POLICY

Author of Policy:	Town Clerk
Date Effective From:	27 October 2020
Policy Review: **When & By Whom**	7 October 2020 Constitution Working Group
Next Review:	September 2022
Version Control:	V2

In accordance with the Freedom of Information Act 2000, this document will be posted on the Council's Website www.spennymoor-tc.gov.uk and copies of this document will be available for inspection on deposit in the Council Offices, Town Hall, Spennymoor. Costs are as per the model publication scheme.

1. Introduction

1.1 This process document lays the framework of responsibility for information risk management across the Council and gives brief examples of what constitutes information governance risk and reporting procedures in the event of information risk breaches.

This document should be considered alongside the Data Security Incident Policy.

2. Key Responsibilities

2.1 **Town Council**: the Town Council will delegate responsibility for the oversight and implementation of information risk management to the Town Clerk who will fulfil the function of Senior Information Risk Owner (SIRO).

2.2 **ICT Working Party (ICT WP):** the ICT WP will, on behalf of the Authority, be responsible for the oversight and assurance of the processes for the identification and assessment of information risk.

2.3 **Senior Information Risk Owner** is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for the Authority. It is their role to:

Oversee the development of this policy and a strategy for implementing the policy within the existing Risk Management and Information Governance Framework.
Take ownership of risk assessment processes for information risk including the review of the annual information risk assessment to support and inform the Annual Governance Statement.
Review and agree actions in respect of identified information risks.
Ensure that the Authority's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
Provide a focal point for the resolution and/or discussion of information risk issues.

2.4 **Information Asset Owners (IAO):** IAOs will provide assurance that information risk is being managed effectively for those information assets that they have been assigned ownership. IAOs will be assisted in their roles by staff acting as Information Asset Administrators or equivalent that have day to day responsibility for management of information risks affecting one or more assets. IAOs will be required to:

Know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset.

Ensure the confidentiality, integrity and availability of all information that their system processes and protect against any anticipated threats or hazards to the security or integrity of such information.

Know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy.

Undertake information risk assessments on all information assets where they have been assigned ownership.

2.5 **Information Asset Administrators (IAA):** IAAs are operational staff with day to day responsibility for managing risks to their information asset and shall work with the IAO and with other supporting staff in risk management roles to manage information risk to their asset.

2.6 **All Staff:** everyone has a role in the effective management of information risk. All staff will actively participate in identifying potential information risks in their areas and contribute to the implementation of appropriate treatment actions.

3. Definitions

3.1 Key definitions are:

Risk: the chance of something happening, which would have an effect on objectives.
Consequence: The outcomes of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
Likelihood: a qualitative description or synonym for probability or frequency.
Risk Assessment: the overall process of risk analysis and risk evaluation.
Risk Management: the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
Risk Treatment: selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:

- Avoid the risk
- Reduce the likelihood of occurrence
- Transfer the risk
- Retain/accept the risk
- Risk Management Process: the systemic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

4. Information Risk Management Process

4.1 **Information Assets**: these come in many shapes and forms. Therefore, the following list can only be illustrative. It is generally sensible to group information assets in a logical manner e.g. where they all relate to the same information system or business process. Typical assets include:

Personal Information Content	Software
• Databases and data files • Back up and archive date • Audit data • Paper records (e.g. patient notes) • Paper reports	• Applications and System Software • Data encryption utilities • Development and maintenance tools
Other Information Content	**Hardware**
• Databases and data files • Back-up and archive data • Audit data • Paper records and reports	• Computing hardware (including PCs, laptops, PDAs, communications devices e.g. blackberry and removable media)
System/Process Documentation	**Miscellaneous**
• System information and documentation • Operations and support procedures • Manuals and training materials • Contracts and agreements • Business continuity plans	• Environmental services (e.g. power and air conditioning) • People skills and experience • Shared service including networks and printers • Computer rooms and equipment • Records libraries

4.2 **Incident Reporting**: Reporting any Serious Incident (SI) relating to actual or potential breaches of confidentiality involving person identifiable data (PID) including data loss will be in line with the Council's Data Security Incident Policy.

5. Monitoring & Review

5.1 The Information Risk Management process will be reviewed at least every two years to identify key areas for continuous improvement.