1 Introduction

This document is part of a set of information governance policies and procedures that supports the delivery of the Information Governance Management Framework (IGMF), it establishes the framework for a formal information risk management programme in the Council by establishing responsibility for information risk identification and analysis, planning for information risk mitigation and information risk management.

Information risk management is an essential element of broader information governance and is an integral part of good management practice. It is therefore the intention of the Council, that information risk management will be embedded throughout all business processes and functions, in the most practical manner possible, that is both 'scalable' and 'proportionate' in the way it is applied. This is aligned, centrally, with the Council's corporate risk management policy and procedures.

It is widely acknowledged that the aim of information risk management is not necessarily to eliminate risk altogether, but to reduce risk by providing a clear structural means to identify, prioritise and manage the risks associate with information. This policy supports these principles by ensuring that all information assets have a clear and appropriate, identified owner and that the risks are regularly assessed and managed.

The policy sets out how information risks will be managed by identifying roles and responsibilities for ensuring the protection of Council assets (including those owned by the Council and those entrusted to it) and by clear risk identification, review, escalation, and treatment processes. Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

This policy should be read in conjunction with the following:

- Information Governance / Data Protection Policy
- Information Security Policy
- Information Security Incident reporting process
- Information Sharing Policy

It also important that the Information Management Strategy is read in conjunction with this policy. If we are to deliver the Information Management Strategy Group's (IMSG) strategic objectives, then we need to approach this more seriously than we have previously.

2 Objective

The information risk management policy has the following objectives:

- To protect the Council, its employers, its partners and its service users from information risks where the likelihood of occurrence and the consequences are significant
- To provide assistance in safeguarding the Councils information assets, consequently providing the needed assurances that statutory and legal requirements relating to information are met.
- To provide an information risk management framework for all Council activities in which information risks will be clearly identified, prioritised accordingly, and considered and addressed through approval, review and control processes.
- To promote and uphold a pro-active approach to information risk management as opposed to reactive.
- To balance the costs of managing and treating information risks with the anticipated benefits that will be derived.

3 Scope

This policy, applies to all CCC information regardless of what format in which it may be held, regardless of wherever it may be held. All contracts for outsourced or shared services must reference the ongoing necessity of full adherence to this policy at all times. There are no exceptions.

4 Policy

This policy:-

- Will define the responsibilities of the IMSG, the Senior Information Risk Owner (SIRO) and the Information Asset Owners (IAOs).

- Demonstrates the commitment of the council towards having robust information assurance arrangements in place.

- Help to ensure that CCC management of information risk is in alignment with best practice recommendations.

5 Management Commitment

Considerable restructuring is taking place across the Council, many directorates are scheduled to move to Friargate in 2017 and it is of imperative importance, to the Council, and to the IMSG, that any restructuring or movement of staff or services, does not place any person identifiable data, sensitive services user or sensitive commercial information at risk of being compromised. As the Council pursues various methods of agile working, it will be an ongoing neccessity to ensure we are fully embedding information risk management into all key controls and approval processess of all business related functions of the Council. This demonstrates the commitment of the IMSG and the senior management and the high level of importance given to minimising information risk and to offer assurance

that we always protect the interests and information, of the public we serve, our Staff members and the Council.

6 Key Documents

A) Information Asset Register (IAR)

The information asset register identifies each information asset held across all areas of the council. It also identifies the Information Asset Owner (IAO), security classification and the importance of the asset. If an information asset recorded in the register is considered to be potentially at risk, the register will detail the information risk status. The IAR is fundamental to the success of information risk management, across the council, and helps to form the basis of the risk assessment work. All IAOs will review the IAR, periodically dependent of information assets held. Typically, this would be in April, July, October, and January unless otherwise agreed with the Senior Information Risk Owner (SIRO).

B) Information Risk Register (IRR)

The information risk register will be a comprehensive record of all identified information risks for the council. It will detail the assessed risk, mitigating action/s, any apparent residual risks, and any outstanding actions for completion. The IAO, accountable for each information asset, will acquire the responsibility, to identify and report the risk and follow through to resolution or acceptance. All IAOs will be expected to submit a quarterly assurance to the SIRO to offer confirmation that all information assets are being appropriately managed and that any information risks have been added to the accordingly to the IRR. The template for quarterly completion by IAOs can be located within the IRR

7 Key Supporting Roles / Responsibilites

Responsibilities

a) Information Management Strategy Group (IMSG)

• Ensures there are adequate information risk management policies and procedures, effectively working and in place for the Council.

• Advising Chief Executive and Senior Management Boards, on information risk management progress as requested.

b) Senior Information Asset Owner (SIRO)

The SIRO is responsible for:-

• Coordinating the development and maintenance of information risk management policies and procedures for the Council via the IMSG.

• Advising Chief Executive and Senior Management Boards, on information risk management strategies and provide periodic reports and briefings on progress.

• Being the owner of the Information Risk Policy, the Risk Assessment procedures and the Information Risk Register.

• Ensuring that there is a mechanism to ensure that an information risk, assessment, and a privacy impact assessment where appropriate, for all new or changed service activities, new deployments of ICT, new contracts and partnership arrangements.

• Ensuring that annual information asset statements from Information Asset Owners are in effect received for all information assets held. To promote and drive best practice in relation to information risk management.

• Monitoring compliance with this Policy including ensuring that there is an Information Security Incident Policy, electronic reporting system and supporting procedures.

• Seek support where required from Internal and External Audit to assess the effectiveness of Information Risk Management

c) Records Manager (RM)

The RM is responsible for:

• Providing Support to the SIRO in undertaking the duties listed above. And ensuring that the SIROs vision and expectations are relayed to all other roles with responsibility for Information Risk.

• Maintaining and controlling the Information Asset Register and Risk Register. Ensuring that both documents are updated regularly and feeding back any areas of non-compliance to the IMSG.

• Supporting Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) in fulfilling their duties in line with this Policy. Offering advice on potential risk treatment and completion of the supporting documentation.

• Help IAOs to identify and apply correct retention periods applicable for records upon request.

• Monitoring compliance with this Policy including ensuring that there is an Information Security Incident Policy, electronic reporting system and supporting procedures.

d) Information Asset Owners (IAOs)

Information Asset Owners are responsible for:

• Ensuring that information risk assessments are performed or reviewed at least once each

quarter on all information assets where they have been assigned ownership and in accordance with the Information Risk Assessment procedures.

• Submitting the risk assessment results and associated mitigation plans to the RM for review.

• Ensuring that for each asset held (considered to be at risk), they will be expected to identify and report the risk via the IRR and IAR and follow through to full resolution or acceptance of that risk by the IMSG / and the Records Manager.

The IAO is accountable to the SIRO and should ensure at all times that arrangements are in place for the completion and thorough maintenance of the IAR, for all assets and to ensure accuracy of the information held at all times. IAOs can identify supporting Information Asset Administrators (IAAs) within their given areas of control, to help manage the workload. Accountability still sits directly with the IAO, regardless of any internal arrangements made.

It is therefore an essential requirement that all IAOs remain actively involved on a day to day basis for managing information assets across their given areas of control.

The IAO is also expected to ensure that:-

- All Information Security Incidents are recorded within '*myservicedesk'* and that Team meetings will have information security incidents, discussed as an ongoing, standing agenda item, moving forwards;

- Where there is a proposed change in *how we are going to work,* that can consequently intrude on the privacy rights of individuals, (Staff or public) – a privacy impact assessment (PIA) screening and assessment, is effectively carried out by working closely with the IG Team to capture and record both the concerns and the solutions needed to protect individuals privacy rights.

- That data/information sharing agreements are effectively in place to govern flows of important information and to ensure that agreements stipulate data sharing that can legitimately taking place, where health and social care information may be held, we must carefully consider the seven caldicott principles prior to sharing.

8 Communication of the Policy

This policy will be communicated,to all staff across the Council via the network of supporting IAOs and IAAs. The policy will be stored within the Information Governance Handbook alongside all other key documentation relating to Information Governance matters. IAOs and IAAs are to ensure that all staff follow this policy at all times.

9. Review

This policy will be subject to annual review by the IMSG.

Document Control:

Version History

Version	Status	Date	Author	Summary of Changes
0.2	TBC	16/12/2016	CR Sadler	NEW POLICY
0.3	TBC	26/01/2016	CR Sadler	Include detailed responsibilities of RM / Agile Working / amend Introduction
0.4	TBC	27/01/2017	CR Sadler	Further edits following consultation
1.0	Approved	07/03/2017	CR Sadler	Further edits *Section 7* key roles and responsibilities (clarity received around information security incident management). *Section 8* communication of the policy delegated to supporting network of IAOs and IAAs

Reviewers

Name	Role	Business Area

Management Approval

Name	Date	Version No.
Lisa Commane	27th January 2017	1.0

Political Approval

Name	Date	Version No.

Distribution

Name	Organisational Department	Format
All	Coventry City Council	Word Document via Intranet