Information Risk Management Policy

Contents:

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supersedes all previous policy on this subject matter.

Information risk management is an essential element of broader information governance and is an integral part of good management practice. It is inherent in all administrative and business activities and all staff are responsible for continuously managing information risk. Information risk management should therefore be embedded into business processes and functions.

It should be noted that this policy complements and applies to the working of the council's Risk Management Strategy, and does not supersede it.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Information Risk Management Policy

Background

The council needs to collect and use certain types of information about its staff, residents, customers and clients in order to carry out its functions, but in doing so needs to ensure that it does this in accordance with the requirements of the Data Protection Act 1998.

The council therefore needs to have a framework to ensure that when new processes, services, systems and other information assets are introduced that the implementation conforms with; Confidentiality, Integrity and Availability (CIA) principles:

Confidentiality: Keeping information safe and secure.

- The privacy and security of information must be maintained. Only those with an legitimate need can access the information and those whose data we are protecting can have confidence in how we safeguard the information.

Integrity: Ensuring information remains accurate and unaltered.

- Having confidence that the information we have is accurate, up to date and free from corruption. This underpins effective decision making and business efficiency.

Availability: Ensuring the information is available to be accessed by authorised users.

- Information must be available to those authorised users at the time and place they need it, so they can effectively make decisions and perform their duties.

This framework sets out a mechanism and behaviours to ensure that information security is properly considered and that any known risks are identified and addressed.

Key Messages

The purpose of this Information Risk Management Policy is to;

- Assist in safeguarding the council's information assets.
- Protect the council, its staff and its customers from information risks where the likelihood of occurrence and the consequences are significant.
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed.
- Encourage pro-active rather than re-active risk management.
- Meet legal and statutory requirements.

Risks

The consequences of poor information risk management may result in;

- Reputational Damage
- Financial Penalties
- Damage to Integrity of information
- Loss of Business and Efficiency

Policy Detail

Documented Information Policies

The council has a number of documented information governance policies and these will be reviewed via the Corporate Information Governance Group on an ongoing basis. All changes to these policies should be formally disseminated to all staff.

Information Risk Register

Any identified information risks will be added included in the Corporate Risk Register which will include the departmental responsibility, the impact and likelihood of the risk, the owner of the risk and the actions being taken to mitigate the risk. Information risks will be captured in the following ways:

a) Risks identified through any procedural changes introduced.

b) Risks identified through formal projects.

c) Outcomes of internal data audits.

d) Risks identified and discussed at the Technical Steering Group.

e) Issues raised at the CIGG.

f) Issues identified by staff.

g) Information Incident management.

h) Any other ad-hoc issues identified by EKS ICT, council staff or customers.

a) Procedural Changes

When the council implements new or changed systems, procedures or contracts, or moves premises, these could affect the way information is stored, processed and shared. Where any changes are planned, it is important that risks to the security of information are recorded and monitored, that the risk is mitigated or accepted, and that a named individual is responsible for these decisions.

All ICT or new system development must firstly be reviewed and approved by the corporate body that exists to oversee systems development. All new projects, including ICT or capital projects must prepare a risk register. Any new risks that are considered of such a nature that they may impact corporate information risks should be submitted to the Office of the SIRO, who will then review these and where appropriate arrange for an update to the Corporate Risk Register.

b) Project Risks

All key projects, including ICT or capital projects must prepare a risk register. Where these are ICT projects the Project Manager must ensure that risks identified through the project review process should be referred to the Office of the SIRO who will assess the risks and add them to the Corporate Risk Register where appropriate.

c) Data Audits/Internal Audits by EKAP

Each service area will undertake data audits in their service area to assess how their data is stored and processed, as well as to detail who has responsibility for the data held and how the data is being managed overall by that service. These data audits will identify areas of risk, and these risks will be assessed by the Office of the SIRO for inclusion in the Corporate Risk Register where appropriate.

d) Technical Steering Group

The Technical Steering Group (TSG) is responsible for the strategic and tactical approach to technology projects and programmes for the three East Kent Districts. This group consists of senior staff from each district as well as EKS ICT staff and is therefore aware of risks that may exist on a strategic and technical level. Where the TSG identifies risks it must ensure that these risks are referred to the Office of the SIRO who will assess the risk and record them on the Corporate Risk Register where appropriate.

e) Corporate Information Governance Group

The Corporate Information Governance Group (CIGG) is responsible for the strategic management and security of data held within the Council. This group consists of the SIROs and senior staff from each of the three East Kent Districts as well as EKS ICT staff and is therefore aware of the actual information breaches that have arisen and the potential risks that could arise in future. Where the CIGG identifies risks it must ensure that these risks are referred to the Office of the SIRO who will assess the risk and record them on the Corporate Risk Register where appropriate.

f) Risks identified by staff

It is often whilst staff are carrying out their normal duties that local or service risks are identified and these are often quite specific. Where such risks are identified these should be referred to the Office of the SIRO who will assess the risk and record them on the Corporate Risk Register where appropriate.

g) Information Security Incidents

All security incidents must be recorded on the council's ICT Information Security Incident Reporting System to ensure that it correctly reported and followed up.

g) Other ad hoc risks identified

All other appropriate issues that are identified by ICT, staff or customers should be referred to the Office of the SIRO who will assess the risk on a case by case basis and record them on the Corporate Risk Register where appropriate.

Review of Information Risks

The information risks included in the Corporate Risk Register will be reviewed six-monthly by the Corporate Management Team who will:

a) Qualify and state these risks so that these are clear.

b) Review the impact and likelihood of existing risks.

c) Agree actions to mitigate and address risks.

d) Undertake actions to address these risks.

e) Decide and Agree on the closure of risks.

Responsibilities

Senior Information Risk Owner

The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises on the effectiveness of information risk management across the Organisation.

The (SIRO) is responsible for co-ordinating the development and maintenance of information risk management policies, procedures and standards for the Council. It is their role to:

- Ensure that the council's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- 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 process to support and inform the Governance Assurance Statement.
- Review and agree actions in respect of identified information risks.

- Provide a focal point for the resolution and/or discussion of information.

Information Asset Owners

Information Assets Owners (IAOs) will provide assurance that the information risk is being managed effectively for those information assets that they have been assigned ownership.

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 working with EKS ICT 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.

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 mitigating actions.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Information Risk Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
	Colin Cook	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review
29/09/2016	Timo Bayford	1.2	CIA definitions added to Background