**Appendix 3**

# Information Security, Risk and Governance Framework

### Introduction

This guidance is aimed at those responsible for managing information security, risk and governance within Canterbury, Dover and Thanet councils. It reflects Government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures within Government'.

The key requirement is for information security, risk and governance to be managed in a robust way within work areas and not be seen as something that is the sole responsibility of ICT or Information Governance (IG) staff. Assurances need to be provided in a consistent manner. To achieve this, a structured approach is needed. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

Information is a valuable asset that each council has a duty and responsibility to protect. We acknowledge our responsibility to our community and the expectations placed on each council where information is concerned. The council understands the duty it has under the Data Protection Act 1998 and is monitored and regulated by the Information Commissioner's Office and the Local Government Data Handling Guidelines. As a local authority, each council will comply with the procedures and requirements of the Local Government Data Handling Guidelines.

The Information Commissioner's Office now have powers to enable them to impose monetary penalty notices to organisations for up to £500,000 and £50,000 to individuals for breaches of the Data Protection Act, along with having the authority to carry out assessments of organisations to ensure their processes follow good practice.

To ensure that information assets and information systems are used and managed effectively, efficiently and ethically, the council has produced an Information Security, Risk and Governance Management Framework, to ensure everyone is aware of their obligations.

### Scope

The Information Security and Governance Policy and all the supporting documents, apply at each council to all employees, Members of the council, temporary staff, contractual third parties, partners or agents of the council who have access to any information, information systems or information assets for council purposes.

## Information Security, Risk and Governance Framework

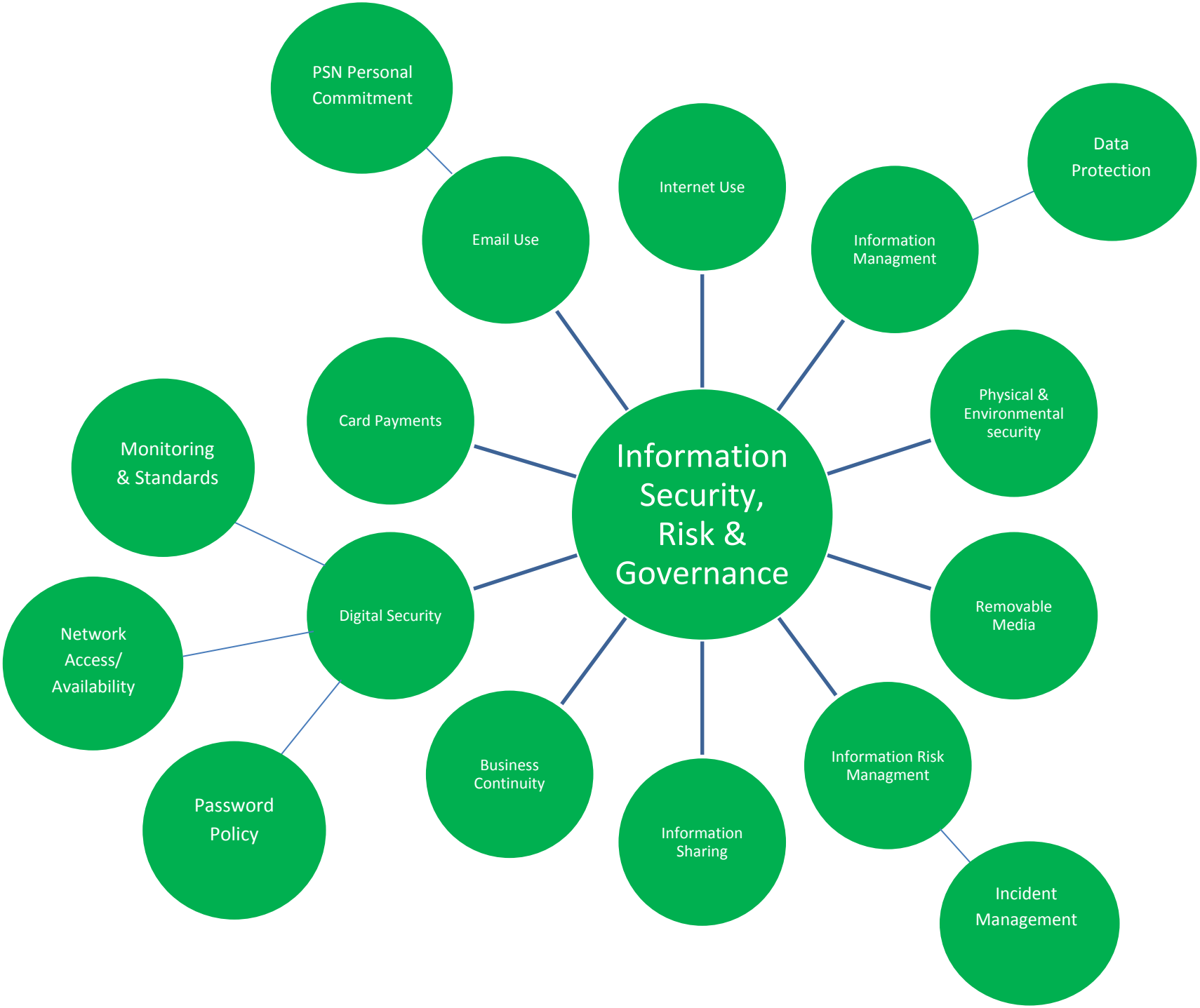
This Information Security, Risk and Governance Policy is the over-arching document of each council's Information Security, Risk and Governance Management Framework, (see figure 1 below). The framework comprises of the Information Security and Governance Policy and specific supporting procedures, standards and guidelines as follows:

1. Internet Use

2. Information Management

    a. Data Protection

3. Password Policy
4. Physical and Environmental Security
5. Removable Media
6. Information Risk Management
    a. Incident Management.
7. Information Sharing
8. Digital Security
    a. Network Access and Availability
    b. Monitoring Standards
9. Business Continuity
10. Card Payments
11. E-mail, instant messaging and social media
    a. Secure e-mail and Public Services Network (PSN)


PSN Personal Commitment
Email Use
Internet Use
Information Managment
Data Protection
Card Payments
Monitoring & Standards
Information Security, Risk & Governance
Physical & Environmental security
Digital Security
Removable Media
Network Access/ Availability
Password Policy
Business Continuity
Information Sharing
Information Risk Managment
Incident Management

## Purpose of the Framework

The purpose and objective of this Information Security, Risk and Governance Framework is to protect the council's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

Each council is committed to protecting information through preserving:

**Confidentiality**

Protecting information from unauthorised access, use and disclosure from unauthorised individuals, entities or processes.

**Integrity**

Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

**Availability**

Being accessible and usable on demand by an authorised individual, entity or process.

## Information/ Information Assets

This Information Security and Governance Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper
- Information or data stored electronically, including scanned images
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- Information stored on portable computing devices including mobile telephones, PDA's and laptops
- Speech, voice recordings and verbal communications, including voicemail
- Published web content, for example intranet and internet
- Cloud and externally hosted data
- Shared data

## Information Asset

This Information Security and Governance Policy also applies to information assets, which come in many shapes and forms. Therefore, the following list can only be illustrative. Typical assets include:

**Personal Information Content**

- Databases and data files.
- Back-up and archive data.

- Audit data.
- Paper records (client case notes and staff records).
- Paper reports.

**Software**

- Applications and System Software.
- Data encryption utilities.
- Development and Maintenance tools.

**Other Information Content**

- Databases and data files.
- Back-up and archive data.
- Audit data.
- Paper records and reports.

**Hardware**

- Computing hardware including PCs, Laptops, PDA, communications devices e.g. I-phones, iPad's and removable media.

**System/Process Documentation**

- System information and documentation.
- Operations and support procedures.
- Manuals and training materials.
- Contracts and agreements.
- Business continuity plans.

**Miscellaneous**

- Environmental services e.g. power and air-conditioning.
- People skills and experience.
- Shared service including Networks and Printers.
- Computer rooms and equipment.
- Records libraries.

## Information Risk Management

Information security and governance arrangements are the overall process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. Information risk management includes physical, personnel and information security and is an essential enabler to making councils work efficiently. Information risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

The council is aware that risks can never be eliminated fully and it has in place a risk strategy that provides a structured, systematic and focused approach to managing risk. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some amount of risk taking is inevitable and necessary if the council is to achieve its objectives.

The council seeks to capitalise on opportunities and to achieve objectives once those decisions are made. By being 'risk aware', the council is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.

Information risk will be managed by assigning roles and responsibilities and co-ordinating the implementation of this policy and all supporting documentation. Together these measures form the Information Risk Management lifecycle and will apply across each council and in their dealings with all partners and third parties.

## Responsibility for Information Risk Management

At each council, Senior Management (Directors and Heads of Service) has the responsibility and accountability for managing the risks within their own work areas. Each council will provide guidance and training to its staff to enable them to understand and carry out their responsibilities in respect of security.

Employees have a duty to work safely, avoid unnecessary waste of resources and contribute to risk management initiatives in their own area of activities. The cooperation and commitment of all employees is required to ensure that council information resources are not unlawfully used as a result of uncontrolled risks.

The Local Government Data Handling Guidelines introduce some specific roles in relation to Information Risk Management as follows:

- Accounting Officer.
- Senior Information Risk Owner.
- Information Asset Owners.
- Support Information Asset Owner.
- System Owner.

These specific roles together with the Data Protection Officer and the IT provider will work together with senior management to ensure compliance with best practice as reasonably practicable with the over-riding objective to keep the council's information safe.

## Role and Responsibilities

The table below details the roles and responsibilities allocated to key staff:

| | |
|---|---|
| **Accounting Officer** | The **Accounting Officer** has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. **(Chief Executive)** |
| **SIRO** | The **Senior Information Risk Owner** is familiar with and takes ownership of the organisation's information risk policy and strategy**. (Nominated Director or Head of Service)** |

| | |
|---|---|
| **IAO** | **Information Asset Owners** are Heads of Service/Managers involved in running the relevant Directorate. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. |
| **SIAO** | **Supporting Information Asset Owners** are at Service Unit Level and may have more familiarity with the information assets of that particular area. They are required to feedback to IAO's on what information their service area holds and how it is being managed. |
| **System Owners** | **System Owners** are responsible for Information systems. They will ensure system protocols are followed. They have responsibility to recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information systems are accurate and up to date. |

The aim is to ensure that the approach to information risk management:

- Takes full advantage of existing authority and responsibility structures where these are fit for this purpose.
- Associates tasks with appropriate management levels.
- Avoids unnecessary impacts on day to day business.
- Ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner.

## 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 Office.

| **Document Control** | | |
|---|---|---|
| **Title/Version** | - | Information Security, Risk and Governance Framework |
| **Owner** | - | Corporate Information Governance Group |
| **Date Approved** | - | |
| **Review Date** | - | |
| **Reviewer** | - | |

| **Revision History** | | | |
|---|---|---|---|
| **Revision Date** | **Reviewer (s)** | **Version** | **Description of Revision** |
| March 2015 | David Randall | 1.0 | Initial Version |
| March 2016 | Hannah Lynch | 1.1 | Format Changes |
| 23/09/2016 | CIGG | 1.2 | Final Review |

| Authority / SIRO | Signature | Date |
|---|---|---|
| Canterbury City Council<br>SIRO | | |
| Dover District Council<br>SIRO | | |
| Thanet District Council<br>SIRO | | |