****

**Information Security Management Policy**

**Approved: v6.0**

**Information Classification: OFFICIAL**

# Introduction

Information is a key asset of Coventry City Council which must be used effectively and lawfully. This policy, and supporting documents within the Information Security Management Framework (ISMF) provide management direction to ensure that the Council's information and ICT assets are appropriately managed. Compliance with this policy will help the Council to efficiently and effectively manage the risks from information security threats.

# Key Policy Statement

Coventry City Council's data and information are key corporate assets. All users have a responsibility for the management and protection of these assets from deliberate, unintentional or unauthorised access, modification, destruction or disclosure.

This policy aims to:

## Preserve confidentiality and privacy rights;

## Maintain accurate and complete information;

## Provide availability to information on a need to know basis at the right time;

## Comply with relevant legislation and regulations.

# Scope

This policy applies to all staff (permanent and agency), Elected Members and third parties and the term ‘user(s)’ will be used throughout this policy to reflect same.

# Policy

## The Council has adopted ISO/IEC 27002:2013 – Code of Practice for Information Security Controls as its baseline for establishing appropriate controls for safe-guarding information.

## The Council will:

## Develop, implement, maintain and monitor an Information Governance Management Framework of policies, standards, procedures and training and awareness material.

## Establish roles and responsibilities for the operational delivery and governance of its information governance requirements and compliance with legislation and standards that are relevant to information governance management.

## Uphold rights to privacy.

## Make available appropriate training and awareness for staff and members

## Implement processes for identifying, investigating and managing risks to information

## Establish, maintain and monitor processes for user access control to ensure only those with a ‘right to know’ have access;

## Actively publish information that can be made public

## Implement specific and appropriate controls for managing third parties who process information on behalf of the Council.

## Maintain the accuracy and completeness of its information assets.

## Implement and maintain business continuity and disaster recovery plans.

# Implementation

## It is the responsibility of all employees to comply with this policy and adopt relevant best practice from the ISMF.

# Training & Awareness

## Awareness and training material will be developed and made available via a combination of techniques.

# Compliance with Policy

## The Senior Information Risk Officer (SIRO) has overall responsibility for Information Security Management in the Council and ensuring that any risks are effectively managed.

## All users who process Council information will be directly responsible for ensuring they have read, understood and comply with this policy and ISMF.

## Compliance with policy and standards may be monitored. Actual and suspected breaches will be investigated and reported to relevant senior management.

# Policy Review

## The Information Governance Team has direct responsibility for co-ordinating the maintenance and annual review of this policy. Reviews will take into account changes in best practice, lessons learnt and input from specialist ICT areas within the Council and in consultation with relevant IT service providers.

## Enquiries regarding this policy should be directed to the Information Governance Team at infogov@coventry.gov.uk or phone (024) 7697 5408.

Document Control:

**Version History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Status | Date | Author | Summary of Changes |
| 1.0 | Approved  | 6/1/03 | R Hall |  |
| 2.0 | Approved | 17/05/05 | A Henninghem |  |
| 3.0 | Approved | 24 August 2009 | J Hutchings |  |
| 4.0 | Approved | March 2015 | J Hutchings | Revised ISO/IEC Standard; removed sections relating to: Other Documents; Risks; Definitions and condensed sections; Council restructure |
| 5.0 | Approved | September 2017 | R Kotonya | Replaced “Security” with “Governance” to reflect terms in ISO 27000 series. Included SIRO responsibility and that policy will be review annual  |
| 6.0 | Approved | November 2021 | S Gilbert | Review of ISO/IEC Standard; replaced “Directorates” with “all employees”; updated IG contact details.  |

**Reviewers**

|  |  |  |
| --- | --- | --- |
| Name | Role | Business Area |
| P Jackson | IT Security Lead Officer | Resources Directorate |
| Information Management Strategy Group (IMSG) |  | All |

**Management Approval**

|  |  |  |
| --- | --- | --- |
| Name | Date | Version No. |
| IMSG | September 2017 | 5.0 |
| Approval not required due to minor updates | June 2022 | 6.0 |

**Distribution**

|  |  |  |
| --- | --- | --- |
| Name | Organisational Department | Format |
| All | Coventry City Council | PDF document via Intranet and Internet |

.