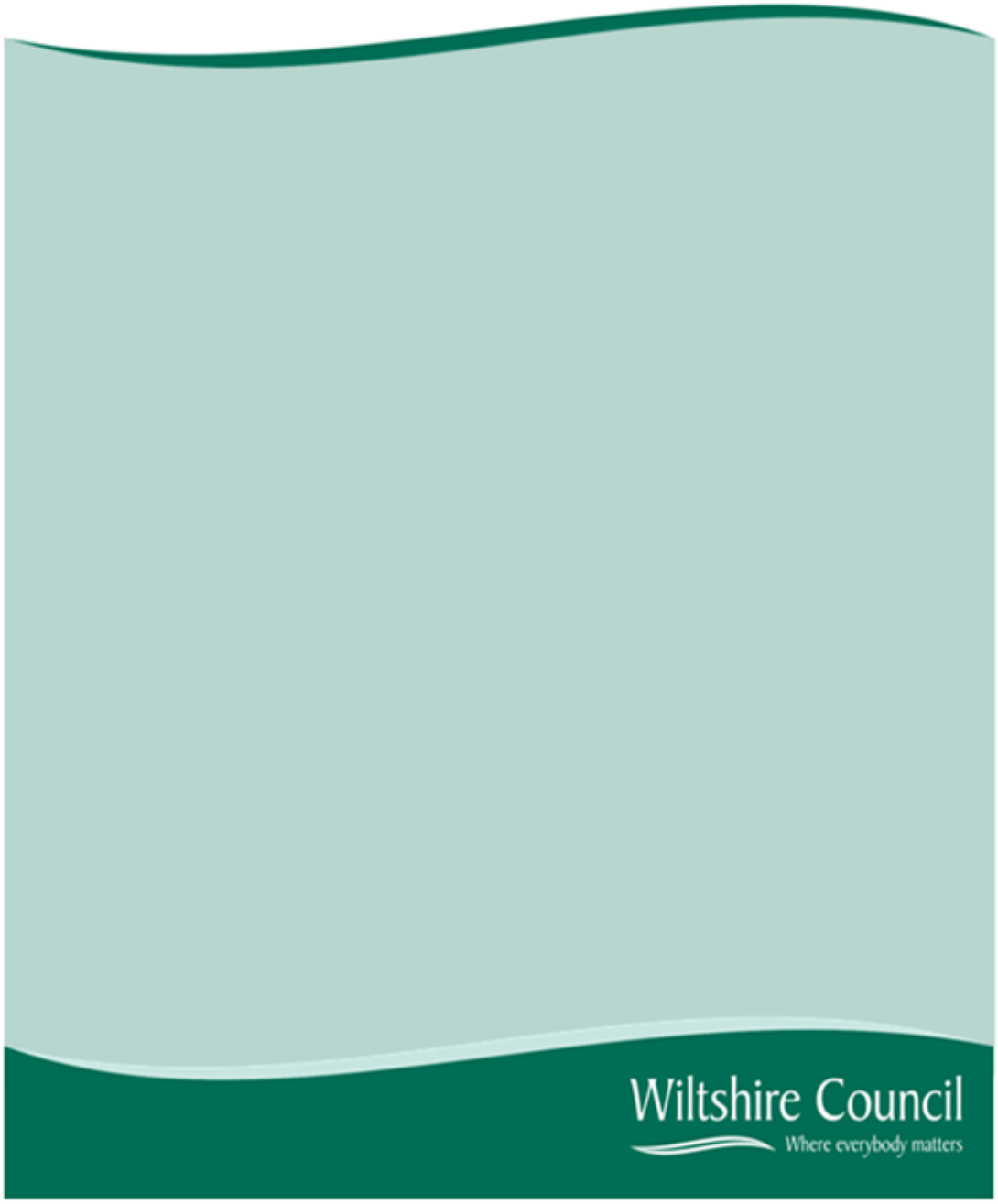
Information Asset Policy



Document Control

Reference Number	**Version** 2.0	**Status** Published	**Sponsor(s)/Author(s)** Tim Way, Sarah Davis-Solan
Amendments	Updates to reflect practice and Information Governance structure		
Document objectives: To establish ownership and accountability for all information assets the Council holds.			
Intended Recipients: All council staff			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators: None			
Training/Resource Implications:			
Ratifying Body and Date Ratified	Information Governance Programme Board September 2017		
Date of Issue	September 2017		
Review Date	September 2018		
Contact for Review	Information Governance		
SIRO signature			

Associated Documentation

Policies

Wiltshire Council controlled documents

- Information security Policy
- Information Governance Policy
- Information Governance Management Framework
- Mobile Working Policy
- Information Asset Change Policy
- Information Security Policy
- Information Incident Management Policy
- Records Management Policy
- Information Classification Scheme
- Network Security Policy

Codes of Practice and Guidance

- ISO 27000:2013 document series relating to information security.
- IG Toolkit https://www.igt.hscic.gov.ukhttps://www.igt.hscic.gov.uk
- PSN Code of Connection (CoCo) https://www.gov.uk/guidance/apply-for-a-public-services-network-psn-connection-compliance-certificate

Contents

1. Introduction

This document sets out mechanisms to protect Wiltshire Council's (the council's) information assets. All information assets must be identified and each must have a responsible owner who is responsible for the maintenance of the required information governance controls.

2. Policy Statement

The purpose of this policy is to provide assurance to the Senior Information Risk Owner (SIRO) and the Corporate Leadership Team that all information held by the council has been identified and appropriate management frameworks are in place to ensure robust information security, information risk management, information business continuity and data quality.

3. Information Assets

An information asset is a body of information, defined and managed as a single unit so that it can be understood, shared, protected and used effectively. Information assets have recognisable and manageable content, value, risk, and lifecycles.

Information assets also include non-computerised systems which hold information. Non-digital assets must be registered with relevant file identifications and storage locations as set out in the council's Records Management Policy.

An information asset primarily consists of the information itself. To effectively manage the asset throughout its lifecycle other factors need to be taken into account:

- Supporting Information – this includes databases, system documentation and procedures, archive media and data;
- Software – this includes application programs, systems, development tools and utilities;
- Physical – this includes infrastructure, equipment, furniture and accommodation used for data processing;
- Services – including computing and communications, heating, lighting, power, air conditioning used for data processing;
- People – including qualifications, skills and experience in the use of information systems;
- Other – for example the reputation and image of the council.

4. Information Asset Register

It is a core information governance objective that all information assets of the organisation are recorded in a comprehensive information asset register maintained by individual Information Asset Owners (IAO) and co-ordinated by the Information Governance (IG) Manager. The information asset register will classify information according to its:

- Criticality to the conduct of council business;
- Level of sensitivity;
- Retention requirements.

Information asset classification must align with the council's Integrated Emergency Management Plan, Information Classification Scheme and Record Management Policy information.

5. Information Asset Role Jobs

IAOs are Heads of Service within the Council.

They are supported by Information Asset Leads (IAL) and specialist staff within the IG team. Accountability rests with the IAO to ensure protection of the information assets within their service. Responsibilities assigned to these roles are set out in in Appendix 1.

Where information assets are shared by multiple parts of the organisation, the IG Manager will determine ownership to ensure there is a clear understanding of responsibilities.

The IAO is expected to understand the overall business goals of the council and how the information assets they own contribute to and affect these goals. The IAO will document, understand and monitor:

- What information assets are held and for what purposes;
- How information is created, amended or added to over time
- Who has access to the information and why;
- Significant risks which may affect information assets.

6. Information Risk

Each IAO is responsible for the risk management and accreditation of the information assets under their control. Accreditation includes completion of:

- Periodic information risk reviews of owned assets;
- Change control notifications for new or modified assets;
- Privacy impact assessments (where deemed necessary by the IG Manager;
- Security evaluations.

7. Data Quality

Access to high quality data is essential for good governance and effective performance management.

Each Information asset must have in place:

- A documented data quality audit plan;
- Audit outcomes to be reported to the IG Manager;
- Local data quality issue logs which are maintained;
- Common issues to be highlighted to the IG Manager for escalation as required;
- Regular data quality spot checks which are formally documented.

8. Business Continuity

Business continuity management (as defined by ISO22301:2012) is:

‘a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.’

Business continuity management is concerned with managing risk to ensure that the organisation can continue operating to a pre-determined minimum level in the event of a major disruption including major IT system failures.

It is the policy of the council to ensure that for all Information Assets:

- Approved Business Continuity plans are in place;
- Relevant staff are notified, and have received training and guidance on the business continuity arrangements;
- Regular testing of business continuity plans is undertaken with outcomes and lessons learned formally reported to the Information Governance Assurance Steering Group (IGASG).

9. Information Security

Information security controls exist to safeguard the confidentiality, integrity and availability of all forms of information with the overall purpose of protecting personal and corporate information from threats.

The implementation and monitoring of security controls at the information asset level ensures comprehensive and consistent information security controls are in place throughout the organisation.

All information assets must be managed in accordance with the council's Information Security Policies.

10. Training

IAOs and IALs must undertake regular training to ensure that they remain effective in their role.

IAOs must ensure that all information asset users undertake approved training for their role and any specific training required for the particular information assets they have access to within their service. Training must incorporate requirements in relation to data quality, information security and risk.

Refresher training will be made available for all staff who have identified training requirements.

All training will be recorded on staff records.

11. Change Control

All changes to information assets (e.g. system upgrades, procurements) must follow the council's Information Asset Change Policy.

12. Information Governance and Audit

The IG Manager will assess compliance against this policy and report any significant issues or risks to the IGASG/SIRO.

IAOs and IALs are required to undertake local compliance spot checks/audits to provide assurance to the Information Governance Assurance Steering Group and the SIRO.

13. Appendix One - Job Role: Senior Information Risk Owner (SIRO)

Purpose of the Role:

The SIRO will implement and lead Information Governance risk assessment and management processes within the council and advise the Board on the effectiveness of information risk management across the Organisation.

Specific Responsibilities:

The key roles of the SIRO are:

- Understand how strategic business goals of the council may be impacted by information risks;
- Acts as an advocate for information risk on the Board;
- Take ownership of risk assessment processes for information risk, including the review of the annual information risk assessment;
- Review and agree actions in respect of identified information risk;
- 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;
- Ensure the Board is adequately briefed on information risk issues;
- The SIRO will be required to undertake strategic information risk management training at least annually.

Associate Directors will be responsible for the following (through their Heads of Service, acting as Information Asset Owners):

- Provide assurance to the SIRO on the security and use of the information assets they are responsible for.
- Take ownership of risk assessment processes for information risk, for their service areas, including the review of the annual information risk assessment.
- Fosters a culture for protecting and using data in their service areas;
- Provides a focal point for managing information risks and incidents.

14. Appendix two - Job Role: Information Asset Owner (IAO)

Under their job descriptions Heads of Service are required to act as the Information Asset Owner for their service areas.

Purpose of the Role:

The IAO's role is to:

- Understand and address risks to the information they 'own';
- Provide assurance to the SIRO on the security and use of these assets.

Specific Responsibilities:

- Maintains understanding of 'owned' assets and how they are used;
- Approves and minimises information transfers while achieving business purposes;
- Approves and oversees the disposal mechanisms for information of the asset when no longer needed;
- Knows what information the asset holds and who has access to update the system;
- Takes visible steps to ensure compliance to the council's Information Governance strategy and action plan;
- Undertakes regular reviews on the information risk associated with the asset;
- Understands and addresses risks to the asset and provides assurance to the SIRO;
- Knows who has access and why, and ensures their use is monitored and compliant with policy;
- Receives, logs and controls requests from other for access;
- Ensures that changes to the system are put through a formal Request for Change process with relevant Equality Impact Assessment, Privacy Impact Assessment, and Information Security Evaluations completed.

15. Appendix three - Job Role: Information Asset Lead (IAL)

Purpose of the Role:

Information Asset Leads will provide support to their IAO to:

- Ensure that policies and procedures are followed
- Recognise potential or actual security incidents
- Consult their IAO on incident management
- Ensure their information asset registers are accurate and maintained up to date.

Specific Responsibilities:

- Ensure compliance with data sharing agreements within the local area;
- Ensure information handling procedures are fit for purpose and properly applied;
- Under the direction of the IAO, ensure that personal information is not unlawfully exploited;
- Recognise new information handling requirements and the relevant IAO is consulted over appropriate procedures;
- Recognise potential or actual security incidents and consult the IAO;
- Report to the relevant IAO on the current state of asset;
- Act as a first port of call for local managers and staff seeking advice on the handling of information;
- Under the direction of the relevant IAO ensure that information is securely destroyed when there is no further requirement for it (Refer to Record Management Policy).