Information Management Governance Framework

Version: 6
Date Issue: November 2018
Review date: November 2020
Reference: WCCC-1073-238
Team: Information Management
Protective Marking: Public

Warwickshire
County Council

Contents

Changes and approvals

v2	Corporate Board	26 November 2014
v3	Information Governance Steering Group (no changes)	9 December 2015
v4	Information Governance Steering Group (changes to organisation)	17 January 2017
v5	Information Governance Steering Group (review for GDPR)	27 March 2018
v6	Information Governance Steering Group (changes to organisation)	20 November 2018

Author: Information Manager and Data Protection Officer

Introduction

Information is a vital asset for the provision of services to the public and for the efficient management of council services and resources. As well as rights to access public and personal information, it plays a key part in governance, service planning and performance management.

"*Governance is about how the County Council ensures it is doing the right things, in the right way, for the right people, in a timely, inclusive, open and accountable manner.*"[1]

Information governance is concerned with how information is held, obtained, recorded, used and shared by the organisation.

Information is used here as a collective term to cover terms such as data, documents, records and content.

It is essential that the council has a robust information governance management framework, to ensure that information is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and adequate resources.

Senior roles

Cabinet and Portfolio Holder

The Cabinet is the lead Councillor body responsible for ensuring governance and decision making within council policies. The Portfolio Holder for Customers and Transformation has specific service responsibilities and this includes information, data protection and IT.

Chief Executive and Corporate Board

The Chief Executive is the Head of Paid Service who leads the council's staff and advises on policies, staffing, service delivery and the effective use of resources. Together with Strategic Directors they form the council's Corporate Board ensuring delivery of an effective council-wide information management approach.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is overall responsible for managing information risk in the council and chairs the Information Governance Steering

[1] Code of Corporate Governance for Warwickshire County Council

Group.

The SIRO:

- fosters a culture for protecting and using information within the council;
- ensures information governance compliance with legislation and council policies;
- provides a focal point for managing information risks and incidents;
- prepares an annual information risk assessment for the council.

Caldicott Guardian

The Caldicott Guardian is responsible for ensuring that all personal/patient identifiable information handled by social care and public health services, are compliant with existing law and standards and they act to safeguard the rights of service users. The Caldicott Guardian ensures that satisfactory information governance policies are in place for their services and adhered to by all staff and providers in their service areas.

Information Asset Owners

Each Assistant Director is an Information Asset Owner who is accountable for information assets within their business unit. They are able to understand how information is held, used and shared and address risks to the information.

Data Protection Officer

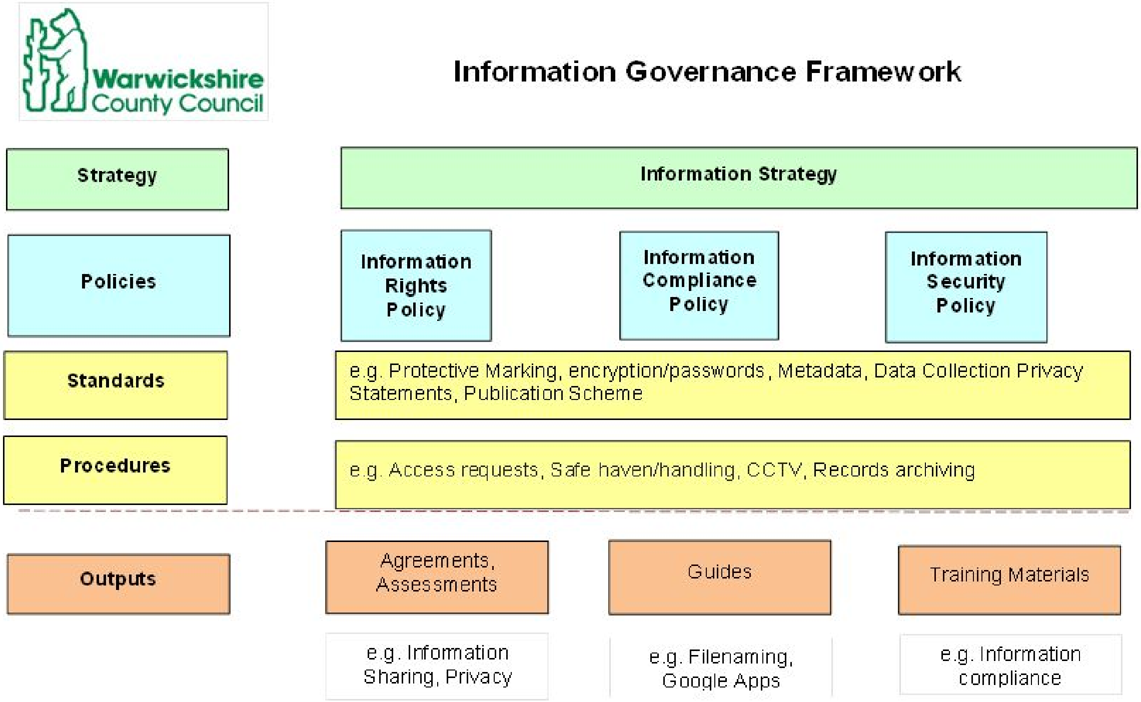
The Data Protection Officer is a statutory role required for all public authorities by the Data Protection Act / General Data Protection Regulation. It is a duty of the council to appoint a Data Protection Officer. They are required to be independent, monitor internal compliance, inform and advise on the council's data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority, the Information Commissioner.

Key policies

The key policies in the framework are the:

- Information Rights Policy – aimed at the public
- Information Compliance Policy – aimed at all staff
- Information Security Policy – aimed at staff and ICT specialist staff

These policies are supported by standards and procedures are shown in the framework diagram. Outputs will be produced from use of these standards and templates, for example privacy assessments, awareness guides and training material. The framework and associated policies, procedures and standards can be found at: www.warwickshire.gov.uk/imframework


Warwickshire County Council
Information Governance Framework
Strategy
Information Strategy
Policies
Information Rights Policy
Information Compliance Policy
Information Security Policy
Standards
e.g. Protective Marking, encryption/passwords, Metadata, Data Collection Privacy Statements, Publication Scheme
Procedures
e.g. Access requests, Safe haven/handling, CCTV, Records archiving
Outputs
Agreements, Assessments
e.g. Information Sharing, Privacy
Guides
e.g. Filenaming, Google Apps
Training Materials
e.g. Information compliance

Key governance bodies

The Information Governance Steering Group (IGSG) responsibility and purpose are to.

- Approve and ensure a comprehensive information governance framework, policies, standards, procedures and systems are in place and operating effectively throughout the council.
- Prepare any annual Information Governance / Risk Assessment required, including action plans.
- Coordinate Information Governance activities (data protection, information requests, information security, quality, and records management) across the council.
- Monitor information handling and breaches, implement assurance controls (including Data Protection compliance audits as required) and take corrective actions
- Ensure training and action plans for information governance are progressed throughout the council and evaluate the impact and effectiveness of governance training.
- Communicate the information governance agenda to staff and the work of the

Steering Group.

The Group comprises of the SIRO, Information Manager & Data Protection Officer, representatives from Cyber Security, Information Management, Legal Services, Facilities Management and each of the Directorates within the council.

Resources

The Information Management team provide expert advice and guidance to all staff on all elements of Information Governance.

- Providing advice and guidance on internal information governance to all staff.
- Developing the Information Strategy, Information Governance Framework of policies, standards and procedures.
- Working with information governance coordinators and service teams to establish protocols on how information is to be used and shared.
- Developing information and data protection awareness and training modules for staff.
- Ensuring compliance with Data Protection, Freedom of information, Records Management, Information Security and other information related legislation.
- Coordinating and processing corporate information requests, processing requests on behalf of business units and supporting information coordinators in other business units.
- Integrating Government and Information Commissioner specific Information Governance guidance, policies and codes of practice.
- Providing support to the Caldicott Guardian and Senior Information Risk Owner for internal Information Governance related issues.
- Completion of audits, compliance assessments and performance.
- Completion of the NHS Data Security and Protection Toolkit.
- Providing support to the Data Protection Officer.

The Cyber Security team is the lead for technical and cyber security management of the infrastructure and technical security advice, including areas such as: Public Sector Network Code of Connection, card security standards (PCIDSS) and device policy.

The Legal Services team provides expert legal opinion on all information governance matters to all service teams, including the Information Management and Cyber Security teams. They also lead on investigating information security incidents.

There will be identified roles in the Groups whose role includes some aspects of information governance and ensuring compliance. These will vary according to the services provided.

Governance framework

Directorate Leadership Teams are accountable for the effective management of information risk and information governance compliance, as well as supporting and promoting the policies, standards and procedures. The teams comprise of the Strategic Director and Assistant Directors for each business unit.

Each **Assistant Director** is an **Information Asset Owner** who is accountable for information assets within their business unit. They are able to understand how it is held, used and shared and address risks to the information. They can delegate responsibility for specific assets to their managers, but not the accountability.

All council **managers** are responsible for the implementation and adherence of this policy and any associated standards and procedures within their service and teams.

Disregard for information governance policies by employees may be regarded as misconduct to which the council's Dismissal and Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal.

Disregard by contractors and agents working for the council will be regarded as a contractual breach. Disregard by volunteers and work experience students working for the council may lead to terminating their work agreement.

Training and guidance

Information Governance training for all staff will be mandatory as part of induction, to include all employees, secondees, agency and voluntary staff. This will be through e-learning modules that are accessible on any device.

Further modules as appropriate to the role will be available through e-learning or classroom session, developed internally or through recognised providers, for example the NHS.

Awareness sessions may be given to staff as required, at team meetings or other events.

Regular reminders on information governance topics are made through corporate and local team briefings, staff news and emails.

Policies, procedures, standards and advice are available to staff at any time on the Information Management pages at: www.warwickshire.gov.uk/im .

Incident management

The Information incident reporting procedure and incident reporting hotline number are available to all staff.

Staff aware of a potential or actual information incident or data breach should report this immediately and within 4 hours. Immediate actions are taken by staff to recover or reduce the risk of loss.

An investigating officer is assigned by the service, and a report completed. Legal Services monitor the investigation and the Incident Group review the final report and put forward recommendations and actions to reduce risk, and agreed by the Head of Service to implement.

For Adult health and social care incidents, the NHS incident procedures will be followed and reported if required, using their reporting tool. Annual figures will be reported via the DSP Toolkit.

Incident performance reports are taken to the Information Governance Steering Group to monitor and agree any corporate actions required.

Monitoring and review

This policy and the supporting standards will be monitored and reviewed annually in line with legislation and codes of best practice.

An Equality Impact Assessment/ Analysis on this policy was undertaken on 27 April 2018 and will be reviewed in April 2021, or before if required.

Further Information

Information Management, Shire Hall, Warwick, CV34 4RL

Web: www.warwickshire.gov.uk/informationmanagement

Telephone: 01926 418633

Appendices

External legislation

Data Protection Act 2018

General Data Protection Regulation

Human Rights Act 1998

Freedom of Information Act 2000

Environmental Information Regulations 2004

Local Government Acts

Copyright, Design and Patents Act 1998

Computer Misuse Act 1990

Common Law

Duty of Confidentiality

This is not a written Act of Parliament. It is “common” law. This means that it has been established over a period of time through the Courts.

It recognises that some information has a quality of confidence, which means that the individual or organisation that provided the information has an expectation that it will not be shared with or disclosed to others.

For information to have a quality of confidence it is generally accepted that:

- it it is not “trivial” in its nature
- it is not in the public domain or easily available from another source
- it has a degree of sensitivity
- it has been communicated for a limited purpose and in circumstances where the individual or organisation is likely to assume an obligation of confidence. For example information shared between a social worker/client, health practitioner/patient, etc.

However, as with the Human Rights Act, confidentiality is a qualified right. The Council is able to override a duty of confidence when it is required by law, or if it is in the public interest to do so.