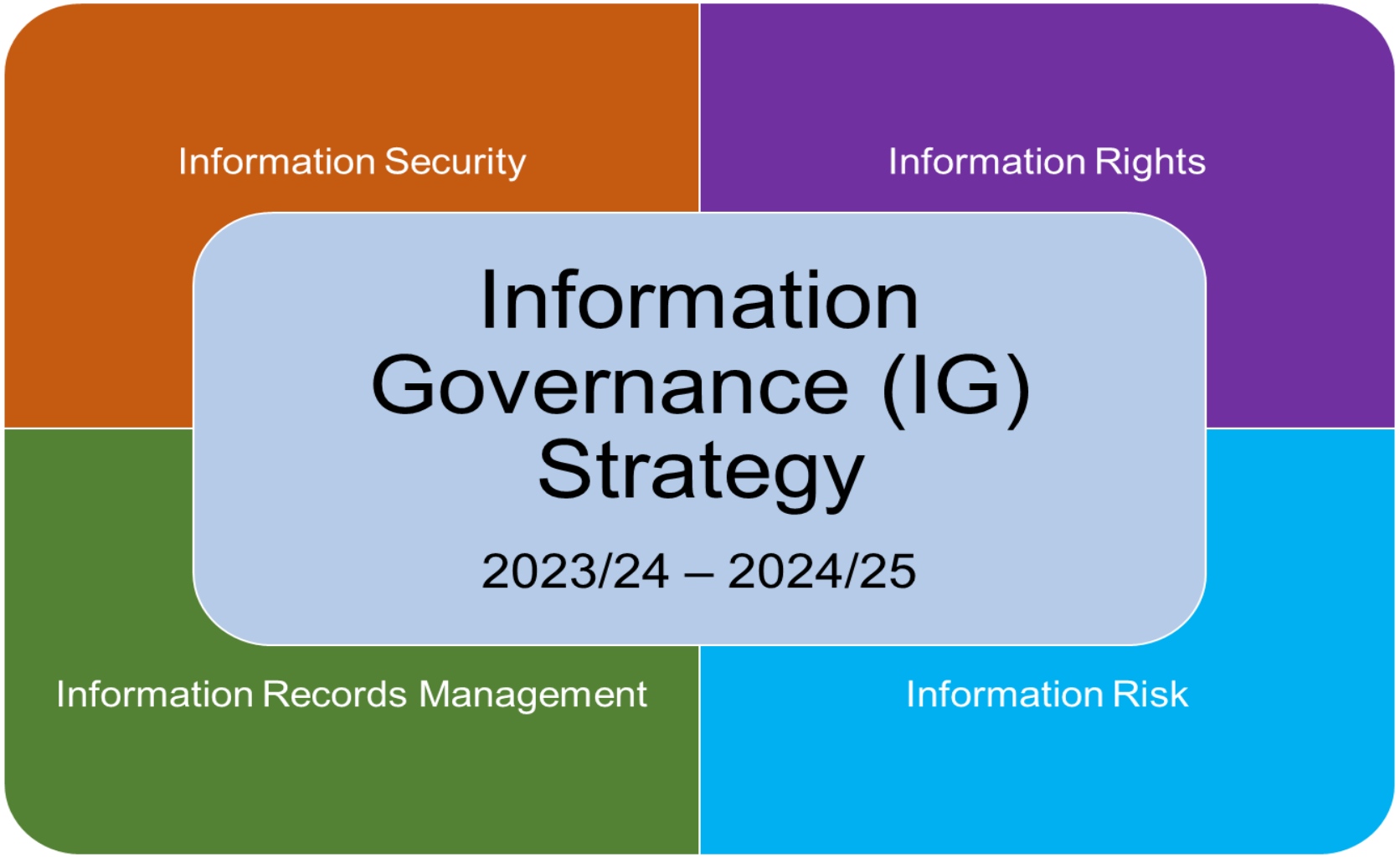
Telford & Wrekin
Co-operative Council

Protect, care and invest
to create a better borough



1. Introduction

1.1 This strategy describes the implementation of a fit for purpose Information Governance (IG) Framework needed for the effective management and protection of organisational and personal information.

1.2 Information Governance describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used by the Council are held, processed and communicated securely and legally.

1.3 Information is a vital asset for the Council, supporting both day to day operations and the effective management of services and resources. Therefore it is essential that all Council information is managed effectively within a robust governance framework.

1.4 In developing this IG strategy the Council recognises and supports:

- The need for an appropriate balance between openness and confidentiality in the management and use of information
- The principles of corporate governance and public accountability but, equally, the importance on security arrangements to safeguard personal information and minimise data breaches
- The need to share customer information with partner organisations and other organisations in a manner consistent with the interests of the customer and where legislation dictates
- The principle that accurate, timely and relevant information is essential to deliver high quality Council services

1.5 This IG strategy sets out how the Council's Information Governance Framework will be implemented and is based on the latest legislation and good practice.

1.6 This strategy will be approved by the Senior Management Team (SMT) and Audit Committee. Approval of IG policies that underpin this strategy will be delegated to the Senior Information Risk Owner (SIRO)[1].

2. Strategic Objectives

2.1 The implementation of this strategy will reflect the Council's Co-operative Values.

Co-operative Value	Linked Information Governance Activity
Openness & Honesty	To proactively publish Council information and make datasets available wherever possible. To respond to information requests made under information rights legislation as required under legislation.
Ownership	Establish clearly defined Information Asset Owners in service areas. To improve the current publication scheme and ensure

[1] This is currently the Director: Policy & Governance

	it continues to meet ICO requirements.
Fairness & Respect	Continue to treat all members of the public requesting information in a consistent and respectful manner.
Involvement	Ensure that the community receives information, both proactively and where requested, that enables them to participate in discussion and challenge the Council where they feel necessary. Make all parties who give/collect information aware of what will happen with the information and give choices in respect to this where legally possible.

2.2 This strategy facilitates organisational, service and SMT development particularly in respect to the appropriate/effective use and management of information to meet the current/future challenges that the Council faces.

3. Leadership and Governance

Strategic Aim –

'SMT proactively engages in leading, championing and monitoring information governance activity across the Council to ensure information governance requirements are embedded in everything the Council does'.

a. Without effective senior level leadership and adequate governance arrangements in place, service areas may experience difficulty in integrating information governance activities in both their medium/long term planning.

3.1 To achieve this strategic aim the following objectives should be met:

REF	Objective
1	Formally establish and embed a number of key information governance roles and responsibilities including: • Senior Management Team/Cabinet Members • Senior Information Risk Owner (SIRO) • Caldicott Guardian *(Officer appointed to develop and maintain responsible, appropriate and secure practices for sharing and handling of personal health and social care information)* • Information Security Group • Information Asset Owners (IAO's) • Audit Committee • Information Governance Specialists See Appendix 1 for expected responsibilities for each of the above
2	SMT to be aware of all key information risks affecting key corporate systems through the risk management process

3	SMT will receive regular reports of progress against information governance strategic aims and objectives
4	IG strategy is aligned to the budget and financial management strategy and other key Council strategies and priorities
5	The IG work programme is drawn up on the basis of risk to ensure finite resources are allocated to add most value to the Council

4 Training, Education and Awareness

Strategic Aim –

'Accurate details of staff IG training are collated and reported to SMT on behalf of the SIRO'.

a. It is important for all Council officers, particularly those with key responsibilities, as detailed in 3.1 above, to be empowered to (and understand their responsibilities) to fulfil the requirements of this strategy and associated information governance policies.

4.1 To achieve this strategic aim, the following objectives should be met:

REF	Objective
1	An IG training plan should exist that meets the needs of the Council and in particular services that process significant volumes of personal and sensitive information.
2	Accurate records are maintained of staff that have completed IG training. Records are collated and reported to the SIRO and SMT.
3	An assessment is made of the coverage and effectiveness of IG training and awareness programme.
4	Specialist training programmes (including information risk management) are in place for staff holding key IG appointments, i.e. those detailed in 3.1 above.

5 Information Risk Management

Strategic Aim –

'Information risk is managed throughout the Council in a structured way so that senior management understand the business impact of IG related risks and manages them effectively'.

a. All officers are responsible for managing information risk.

b. The SIRO has a corporate responsibility for providing a focal point for information risk management. The SIRO does not fulfil this responsibility personally but delegates responsibility to Managers and Information Asset Owners across the Council.

5.1 To achieve this strategic aim the following objectives should be met:

REF	Objective
1	The SIRO/SMT will be aware of key information risks affecting systems through the risk management process.
2	The SIRO will ensure proportionate processes are in place to ensure information risks

	are mitigated.
3	The Council and external organisations who share information with each other should be satisfied with the level of risk exposure relevant to this sharing.
4	Key information risk vulnerabilities common to more than one system are assessed and communicated corporately.
5	Data Protection impact assessments (DPIA) are undertaken for all new information systems that process personal information.
6	The SIRO/SMT determine the risk appetite for information.
7	Processes are in place to conduct operational and technical risk assessments of information systems and associated policies/processes.

6 Life Cycle of Information

Strategic Aim –

'A full range of information governance measures should be implemented that are cost effective and reduce the vulnerability to information security issues/breaches throughout the life of the use of information and its eventual destruction'.

a. Employees who handle information should understand the full process for managing this information from collection through to retention, sharing and disposal.

6.1 To achieve this strategic aim the following objectives should be met:

REF	Objective
1	Reviews are undertaken on the status of information governance control measures that impact all key information system and information assets. The results of reviews are made available to the SIRO and SMT.
2	Processes are in place to map information governance incidents and key vulnerabilities against relevant service areas.
3	Appropriate back up, business continuity and disaster recovery arrangements are in place and have been tested for all information systems.
4	A digital continuity risk plan is in place that encompasses an annual review of all information assets.
5	Contracts with third party suppliers detail conditions in respect to digital continuity.
6	A scaleable and future proofed authentication method (access controls) is in place for all information systems.
7	A plan is in place for the prevention, detection, and resolution of information governance vulnerabilities including suitable penetration testing
8	A patching policy is in place that includes third party suppliers and details the distinction between routine, critical and emergency patching. It also includes the requirements for information on malware incidents to be collated and reported
9	A corporate information retention schedule is established, embedded and complied with by all Council services

7 Assured Information Sharing

Strategic Aim –

'Information is shared legally within the Council and with external bodies / individuals in an assured and cost effective way that maximises the benefits delivered by sharing information whilst reducing the business impact should information be shared inappropriately'.

a. Information sharing is an essential part of Council business. It allows more efficient, joined up services to be delivered to the community by the Council and/or strategic partners to benefit customers receiving these services. However sharing information can lead to vulnerabilities particularly if it is not being undertaken in a controlled and managed way.

7.1 To achieve this strategic aim the following objectives should be met:

REF	Objective
1	Information sharing agreements should be in place with third party organisations where regular sharing occurs
2	Mechanisms are in place to protect information in transit
3	Plans for a protective marking scheme for all information assets
4	Agreed Council policies are in place in respect to information sharing

8 Compliance

Strategic Aim:

'Effective compliance mechanisms provide positive assurance that Council policies are being implemented in an effective way to achieve the desired outcomes'.

a. Without an effective compliance programme, IG controls which manage information risks (sometimes causing perceived inconvenience) are likely to be ignored resulting in an increase in the risk to the Council's information.

8.1 To achieve this strategic aim the following objectives must be met:

REF	Objective
1	The SIRO is satisfied that the Council is complying with relevant IG legislation
2	A compliance programme is in place that has been agreed by the SIRO and progress against completion is regularly reviewed
3	Weaknesses identified from compliance reviews are rectified with lessons learnt being reported to the SIRO and SMT

Appendix 1

Formally establish and embed a number of key roles and responsibilities including:

- **Senior Management Team/Cabinet Members** – provides the correct leadership for the Council in relation to information governance reinforcing the importance of effective information governance in every aspect of Council business
- **Senior Information Risk Owner (SIRO)** – A member of SMT who is accountable for
    - Fostering a culture for protecting and using data
    - Providing a focal point for managing information risks and incidents
    - Is concerned with the management of all information assets.
- **Caldicott Guardian** – Develop and maintain responsible, appropriate and secure practices for sharing and handling of personal health and social care information.
- **Information Security Group** – Group includes a number of key officers in the Council and is chaired by the Audit & Governance Team Leader. The group's remit is to discuss and monitor information security/governance issues and compliance across the Council and report significant issues to SMT.
- **Information Asset Owners (IAOs)** – All service areas have information assets, some have more than others. The IAO is responsible for ensuring information assets in his/her area are adequately protected/risk assessed, managed under statutory obligations and that their value to the Council is fully exploited
- **Audit Committee** – The Audit Committee seeks assurance that the Council's governance processes including the information governance processes are operating properly.
- **Information Governance (IG) Specialists** – IG specialists provide a number of key functions including:
    - Advice and support to the Council in respect to all information governance matters
    - Co-ordinating all information requests received under information rights legislation
    - Checking for corporate compliance in conjunction with Internal Audit with agreed information governance policies and procedures

Document Version Control

Version	Date	Author	Sent To	Comments
V4	29/4/19	R Montgomery	CISG	Updated strategy for next 3 years
V5	22/11/19	R Montgomery	Kirsty King, Anthea Lowe and Jonathan Eatough	Updated strategy for next 3 years for comment.
V6	27/3/23	R Montgomery	Kirsty King	Updated strategy for next 2 years
V6.1	3/4/23	R Montgomery	Anthea Lowe	Amended version including comment from K King. Sent to AL for comment
V6.2	14/4/23	R Montgomery	Corporate	Updated version includes K King and A Lowe comments