Information Security and Governance Policy and Framework

Contents

1. Information governance

1.1. Summary

The information governance policy sets the high-level direction and required standards across the organisation. This is supported, where necessary, by specific system and area policies, where the required controls are explained in detail.

1.2. Why is this important?

Information is one of the Council's most valuable assets. It underpins effective service delivery, supports decision-making, helps manage resources, and drives continuous improvement.

To protect this asset, we must manage information properly and securely. This means having clear policies, procedures, and responsibilities in place—ensuring everyone understands their role in maintaining high standards of information governance.

Information governance is the framework we use to handle information about our residents, employees, and partners—especially personal or sensitive data. It ensures we comply with legal obligations like the General Data Protection Regulation (GDPR) and the Freedom of Information Act (FOIA), and follow best practice from government and regulatory bodies.

Good information governance brings together data protection, access to information, data quality, and both digital and physical security. It helps us to be transparent, accountable, and trusted by the people we serve.

1.3. Scope

This policy covers all aspects of information within the organisation, including (but not limited to)

- service user information
- staff-related information
- organisational information
- Information held by third parties and other organisations on behalf of the Council

1.4. Strategy

The Council's information governance strategy sets out how we protect, manage, and use information effectively and securely. It ensures we meet our legal obligations, support transparency, and maintain public trust.

Our approach is built around the following key elements:

- **A clear policy and governance framework**: The Council's Information Security and Governance Policy defines how information is managed and protected across all services.

- **A rolling improvement plan**: This is regularly updated based on internal assessments and benchmarks, including relevant national standards such as the NHS Data Security & Protection Toolkit where appropriate.

- **Training and awareness**: All staff are required to complete annual data protection and cyber security training. A programme of ongoing training and guidance is maintained and overseen by the Corporate Information Governance Group to support a strong culture of accountability and best practice.

- **Performance monitoring**: Information governance performance is tracked and reported at the Corporate Information Governance Group . Where relevant, this includes annual submissions to external regulators, and audits by internal and external reviewers.

- **Continuous improvement and assurance**: The strategy, along with supporting policies and action plans, is reviewed annually to ensure it remains effective, responsive to emerging risks, and aligned with best practice.

By embedding these principles, we aim to ensure that information is managed securely, used appropriately, and shared responsibly across the organisation.

1.5. Key Principles

There are four key principles related to the Council's information governance policy:

- openness
- legal compliance
- information security
- quality assurance

1.5.1 Openness

The Council is committed to being open and transparent in how it operates, makes decisions, and delivers services. To support this principle, we will:

- Make non-confidential information about our services, decisions, and performance publicly available, in line with the Council's Transparency Code and obligations under the Freedom of Information Act.

- Ensure individuals can access their personal data through the Subject Access Request process, supported by clear guidance and accessible procedures.

- Maintain clear and responsive channels for handling enquiries from residents, stakeholders, and the media.

- Regularly review and assess our openness and transparency arrangements, including through internal audits or independent assessments where appropriate.

Promoting openness builds trust, strengthens accountability, and helps residents understand how the Council serves their community.

1.5.2 Legal compliance

The Council is committed to handling all information in accordance with the law. To ensure legal compliance, we will:

- Treat all personal and sensitive information as confidential, unless disclosure is required by law or aligns with national policies on transparency and accountability.

- Conduct regular assessments and audits to monitor compliance with relevant legal and regulatory requirements.

- Maintain up-to-date policies and procedures to ensure we meet our obligations under data protection legislation, including the UK GDPR, Data Protection Act 2018, the Human Rights Act, and common law duties of confidentiality.

- Put in place appropriate data sharing agreements with external organisations to ensure any sharing of personal information is lawful, proportionate, and clearly justified – in line with relevant data protection and information sharing legislation.

Maintaining legal compliance is essential to protect individuals' rights, uphold public trust, and ensure accountability in how the Council manages personal and confidential information.

1.5.3 Information security

The Council is committed to protecting the confidentiality, integrity, and availability of the information it holds. To maintain high standards of information security, we will:

- Maintain clear policies and procedures for the secure handling, storage, and management of all information assets and ICT systems.

- Carry out regular assessments and audits of our information security and ICT controls to identify risks and ensure compliance.

- Promote a strong culture of confidentiality and data protection through staff training, guidance, and awareness campaigns.

- Operate robust incident reporting procedures, ensuring all actual or suspected security breaches are logged, investigated, and addressed appropriately.

Effective information security protects individuals' data, maintains public trust, and ensures that the Council continues to deliver services safely and securely.

1.5.4 Quality assurance

The Council is committed to maintaining high standards of information quality and effective records management. To support this, we will:

- Maintain clear policies and procedures to support information quality and accurate record-keeping.

- Conduct regular assessments and audits of information quality and records management practices.

- Require managers to take responsibility for the accuracy and reliability of information within their services.

- Ensure, wherever possible, that information is accurate and complete at the point of collection.

- Apply consistent data standards in line with recognised best practice.

- Support staff with guidance, training, and resources to promote good information quality and records management.

1.6. Related policies

- Acceptable Use Policy
- Records Management
- Information Classification and Marking
- Information Security Incident Reporting
- Information Security Risk Management Policy
- HR policies relating to an individual's job employment, role and responsibilities (ie screening, terms and conditions of employment, disciplinary action etc)
- the Council's Code of Conduct

1.7 Legal and Regulatory Framework

The Council must comply with a wide range of legislation, regulations, and best practice standards that govern how information is collected, used, stored, and shared. Key legal and regulatory requirements include:

- **UK General Data Protection Regulation (UK GDPR)** and **Data Protection Act 2018** – governing the use of personal data.
- **Freedom of Information Act 2000** – providing public access to information held by public authorities.
- **Environmental Information Regulations 2004** – relating to environmental data.
- **Human Rights Act 1998** – ensuring respect for individuals' private and family life.
- **Common Law Duty of Confidentiality** – applying to personal and sensitive information.
- **Computer Misuse Act 1990** – protecting against unauthorised access to information systems.
- **Public Records Act 1958** and **Local Government Act 1972** – setting standards for recordkeeping and access to information.
- **Re-use of Public Sector Information Regulations 2015** – supporting transparency and re-use of non-personal data.
- **Regulation of Investigatory Powers Act 2000 (RIPA)** – governing the lawful interception and monitoring of communications.

Where relevant, the Council also adheres to sector-specific legislation and professional codes of practice, including requirements relating to health and social care, national security, and safeguarding.

The Council also recognises frameworks and standards such as the **Caldicott Principles**, the **NHS Data Security & Protection Toolkit**, and compliance with requirements for secure connectivity (e.g., **Public Services Network**, **NHS Data Exchange**).

1.8. Review and evaluation

The Corporate Information Governance Group is responsible for the maintenance and review of this policy. Legal and statutory responsibility for information governance rests with the Council's:

- **Senior Information Risk Owner (SIRO)**
- **Caldicott Guardians** (for health and social care data)
- **Data Protection Officer (DPO)** (for data protection compliance and liaison with the ICO)

This policy will be reviewed:

- Every 2 years as part of the Council's governance cycle
- Following any major breach or incident
- When new threats or vulnerabilities are identified
- After significant changes to organisational structure or technical infrastructure

Evaluation methods may include:

- Completion of the NHS Data Security and Protection Toolkit
- Accreditation or compliance checks (e.g., Public Services Network)
- Internal and external audit programmes

Evaluation criteria may include:

- Number and severity of reported breaches
- External assessments and compliance ratings
- Staff awareness and training participation
- Evidence of leadership commitment and ongoing improvement

1.9. Responsibilities

Effective information governance relies on clearly defined responsibilities across the organisation:

a. Coordination and Oversight

The **Corporate Information Governance Group** is responsible for the strategic coordination of information governance activities across the Council.

b. Information Asset Ownership

Each information asset must have an assigned **Information Asset Owner (IAO)**—typically a director within the relevant service—who is responsible for its security, access controls, and compliance. IAOs work closely with information governance leads and system managers.

c. System Management

System owners are accountable for:

- Managing and authorising user access
- Implementing audit and activity monitoring
- Ensuring data validation and accuracy
- Overseeing third-party support where applicable

d. SIRO and Caldicott Guardian

The **Senior Information Risk Owner (SIRO)** and **Caldicott Guardians** oversee the governance of personal and sensitive information, particularly where person-identifiable data is used or shared. This includes:

- Establishing access procedures and protocols
- Reviewing data sharing with external organisations
- Aligning local practices with national guidance

e. Data Protection Officer (DPO)

The DPO is responsible for:

- Advising the Council on compliance with data protection legislation (including UK GDPR and the Data Protection Act 2018)
- Monitoring implementation of data protection policies and training
- Supporting and advising on Data Protection Impact Assessments (DPIAs)
- Acting as the contact point for data subjects and the Information Commissioner's Office (ICO)
- Reporting independently on the Council's data protection performance to senior management

f. Information Security

Information Security & Governance Policy and Framework

The Council's **shared Digital & IT service** leads on ICT security, including:

- Development of Digital & IT security policies
- Promotion of good security practices
- Ensuring PSN (Public Services Network) compliance and audit readiness

g. Records and Document Management

The Digital & IT service also leads on implementing systems and practices that ensure compliance with:

- Data protection legislation (UK GDPR, DPA 2018)
- Freedom of Information Act
- Records management codes of practice

h. Physical Security

Facilities Management, supported by service managers, is responsible for maintaining physical security of Council buildings. All staff are responsible for ensuring the physical security of the information they handle.

i. Line Management and HR

Managers must:

- Ensure staff receive appropriate training
- Promote and monitor compliance with relevant policies
- Take action where non-compliance occurs

j. Staff Responsibilities

All Council staff are expected to maintain confidentiality and follow information governance policies. Temporary staff, contractors, and third parties must sign confidentiality agreements before accessing Council systems or data.

1.10 Training and Awareness

Information Security & Governance Policy and Framework

All staff are required to complete **annual Data Protection and Cyber Security training**, covering information security, data protection, and acceptable use.

Additional training is required for staff in specialist roles, such as:

- Data Protection Officer (DPO)
- SIRO
- Information Asset Owners
- Caldicott Guardians

Directorates may provide induction training tailored to their specific service requirements. An up-to-date intranet resource is maintained to support staff understanding and compliance.

1.11 Information Sharing with Other Organisations

The Council regularly shares information with external partners to support effective service delivery. Information sharing is governed by:

- An overarching **Information Sharing Protocol**, where applicable
- **Purpose-specific agreements**, in line with data protection law
- **Data Protection Impact Assessments (DPIAs)** for new or high-risk data sharing

All data sharing must be lawful, proportionate, and clearly justified. A consistent approach to developing and approving data sharing agreements will be maintained across the Council.

2.1 Summary

All staff and users of the Council's ICT and related services have a duty to protect the systems, information, and data they access or manage. This policy outlines the importance of information security and the roles of the Corporate Information Governance Group and senior staff in ensuring Council employees understand their responsibilities.

2.2 Why is this important?

Information is essential to the Council's effective operation and must only be used for its intended purpose—supporting Council services. The objectives of this policy are to:

- Protect the Council's information assets, ensuring their availability and integrity
- Maintain the privacy and trust of our users by safeguarding their information and complying with applicable laws, regulations, and third-party agreements

- Ensure any shared information is protected against unauthorised access and managed according to this policy and any relevant sharing agreements or protocols

- Support the Council's accreditation with third-party frameworks, including the Public Services Network (PSN) and NHS Information Governance Toolkit

- Require prompt reporting, thorough investigation, and appropriate response to all actual or suspected information security breaches to prevent recurrence

This policy should be read alongside the Council's **Acceptable Use Policy**, which sets out the standards for appropriate and secure use of ICT systems.

2.3 Scope

This policy applies to everyone who uses or accesses the Council's information assets and ICT resources, including but not limited to:

- Permanent staff
- Temporary staff
- Councillors
- Third parties such as suppliers, partners, work-experience placements, and students

2.4. Key Principles

The Council's Information Security Policy is based on six core principles:

- **Information** — managing data as a valuable asset
- **Confidentiality** — ensuring information is only accessible to authorized individuals
- **Integrity** — maintaining accuracy and completeness of information
- **Availability** — ensuring information and systems are accessible when needed
- **Authentication and Access Control** — verifying identities and managing permissions
- **Auditing** — monitoring and recording activity to detect and respond to incidents.

2.4.1 Information

Information is a valuable asset and will be protected in accordance with all relevant laws, regulations, and any data sharing agreements the Council has in place.

2.4.2 Confidentiality

The Council must ensure that proprietary, personal, and client information is only accessible to authorized individuals.

2.4.3 Integrity

The accuracy and completeness of information must be maintained. Any changes must be authorised, controlled, and validated through established business processes.

2.4.4 Availability

Information and critical systems must be accessible to authorised users when needed. Disaster recovery and business continuity plans must be developed, maintained, tested, and regularly reviewed to ensure recovery from incidents or attacks.

2.4.5 Authentication and Access Control

Access to Council information and systems must be authorised and linked to individual user accounts. Access rights are limited strictly to what is necessary for each person's role. External users, such as customers or businesses, may only access information about themselves after identity verification.

2.4.6 Auditing

User activity across Council IT systems, including computers, firewalls, and networks, will be logged and retained in line with security policies, legal, and regulatory requirements. These logs will be available for review as necessary.

Security policies, processes, and procedures supporting these principles are maintained and accessible to staff via the Council intranet.

2.5. Review and evaluation
The information security policy will be assessed against the following criteria:

- review of information security incidents through regular reports to the Corporate IG Group
- applicable controls to be audited at least once every three years
- internal audits to be carried out periodically
- business continuity plans to be tested annually
- records demonstrating the completion of security training both as part of employee/ contractor induction, and as an ongoing annual requirement

2.6. Responsibilities
Information security responsibilities include:

Overall responsibility
The Council's Chief Executive is ultimately responsible for the protection of information.

Security policies
The Director of Digital and ICT is responsible for maintaining information security policies, which are reviewed every 2 years by the Corporate Information Governance Group.

Information governance coordination

Information Security & Governance Policy and Framework

The Corporate Information Governanc Group is responsible for the implementation of this policy, and for the development, maintenance and promotion of relevant information security policies, procedures and guidance.

Training
The Corporate IG Group is responsible for ensuring appropriate training on information security is made available to staff. Managers are responsible for ensuring that staff complete the training.

Protection and control
Information Asset Owners are responsible for identifying and ensuring that all information used by their service is appropriately protected and controlled. They are responsible for implementing the security policies within their areas, and for ensuring staff adhere to these.

Caldicott Guardian
The Caldicott Guardian is a senior officer responsible for overseeing the lawful, ethical, and appropriate use of personal information specifically in relation to adult social care and public health services. The role focuses on ensuring that information is handled in a way that maintains confidentiality and supports appropriate data sharing, both within the Council and with external organisations.

The Guardian plays a key advisory role in safeguarding service user information and ensuring compliance with confidentiality principles, particularly where there are complex or sensitive data-sharing decisions.

Further details of the role and its responsibilities are outlined in *The Caldicott Guardian Manual 2017*, published by the Department of Health and Social Care.

Role of the information asset owner (IAO)
Information asset owners are senior/responsible individuals involved in running the relevant business. At Kingston Council the Corporate Heads of Service are the responsible Information Asset Owners.

Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good. Information Asset Owners lead and foster a culture that ensures information is valued, protected and used appropriately.

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

Document and records management
IAOs are responsible for ensuring there is a record management (archiving, deletion, destruction) policy in place for both manual and electronic information held by their service.

Security breaches
All breaches of information security (actual or suspected) must be reported following the process on the intranet. Which is to report to the Information Governance Team via a Google form.
Where an information security incident may breach the Council's information security policies and/or other Council policies and could lead to disciplinary action, then the investigation will be conducted in line with Council disciplinary rules and procedures.

Data Protection Impact Assessments (DPIA)
All new projects and significant changes to existing systems, applications, or the ways we use personal information that are likely to result in a high risk to individuals' rights and freedoms must be subject to a DPIA. This assessment ensures that potential privacy impacts are identified, evaluated, and mitigated, thereby protecting the Council's information assets and the personal data we hold

General staff
All staff (permanent, temporary and those employed by third party suppliers) are responsible for the information they access and use. In line with this, it is their responsibility to understand and adhere to the Council's information security policies.

2.7. Training
All members of staff are required to complete information security and governance refresher training on an annual basis. In addition:

- senior Council staff, and those with roles specifically related to information governance (eg SIRO, Information Asset Owner, Caldicott Guardian etc) are required to complete additional training as appropriate
- directorates may hold their own induction training to cover service-specific requirements of that directorate.
- the intranet is maintained as an up-to-date resource for all staff to use

3. GDPR Compliance

The Council has a robust and effective data protection framework in place that ensures compliance with data protection law, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This framework supports accountability, transparency, and the safeguarding of personal data across all services.

3.1 Data Retention and Disposal

Retention and disposal of personal data are managed in line with agreed schedules to support the principles of data minimisation and storage limitation. These schedules ensure that personal data is retained only as long as necessary and is securely disposed of when no longer required.

3.2 Data Breaches

We have a clear and accessible data breach response procedure, which sets out the steps for identifying, reporting, investigating, and resolving information security incidents involving personal data. Staff are trained to follow this process, which is available on the Council's intranet.

3.3 Data Subject Access Requests (SARs)

Individuals have the right to request access to their personal data. Our SAR process complies with statutory timescales and requirements, including the one-month response period and provision of data free of charge (subject to exemptions). Guidance for staff is available on the intranet.

3.4 Legal Basis for Processing

All data processing activities are regularly reviewed to ensure they are lawful, fair, and transparent. Legal bases for processing are documented within our Record of Processing Activities (ROPA) in accordance with Article 30 of the UK GDPR.

3.5 Consent

Where consent is used as the legal basis for processing, it is obtained through clear, informed, and affirmative opt-in mechanisms. Consent is never bundled with other terms and is recorded appropriately. Individuals are informed of their right to withdraw consent at any time.

3.6 Privacy Notices

We maintain up-to-date privacy notices that explain why we collect personal information, how it is used, the lawful basis for processing, who it may be shared with, and what rights individuals have. Privacy notices are available on our website and provided at the point of data collection.

3.7 Data Subject Rights

We promote awareness of individual rights under the UK GDPR through accessible information on our website and internal platforms. These rights include:

- Access to personal data
- Rectification of inaccurate or incomplete data
- Erasure ('right to be forgotten') where applicable
- Restriction or objection to processing
- Data portability (where applicable)
- Not to be subject to automated decision-making without safeguards
- The right to lodge a complaint with the Information Commissioner's Office (ICO)

Support for exercising these rights is available through the Council's Data Protection Officer (DPO) and designated service contacts.

4. Role of the Corporate Information Governance Group (CIGG)

The Corporate Information Governance Group (CIGG) provides strategic oversight and coordination of the Council's information governance and cyber security. It ensures visible ownership, clear direction, and senior management support for compliance across all services.

CIGG is responsible for:

- Setting the strategic direction for information governance and cyber security, supporting the work of the Data Protection Officer (DPO), Senior Information Risk Owner (SIRO), and Caldicott Guardian.

- Monitoring and enforcing compliance with data protection law (including UK GDPR and the Data Protection Act 2018), Freedom of Information (FOI), Environmental Information Regulations (EIR), and relevant information security standards (e.g. the Cyber Assessment Framework).

- Developing, reviewing and approving corporate policies, procedures, and frameworks related to information governance and information security.

- Identifying and managing risks related to data protection, information security, and information governance, and ensuring appropriate controls are in place to mitigate these.

- Promoting awareness and good practice in data protection and cyber security across the organisation.

- Overseeing the reporting and investigation of information security incidents and personal data breaches, including those that require escalation to the ICO or the Council's Senior Leadership Team (SLT).

Membership includes:

- Chair: General Counsel / Monitoring Officer

- Data Protection Officer (DPO)

- Senior Information Risk Owner (SIRO)

- Caldicott Guardian

- Head of Internal Audit

- Representative(s) from Digital & IT

Meeting arrangements:

- CIGG meets quarterly and is chaired by the General Counsel.
- Meetings are organised by the DPO, who circulates an agenda and papers five working days in advance.
- Members who are unable to attend must nominate a deputy.
- The group's Terms of Reference are reviewed every 2 years.

Standing agenda items include:

- Performance updates (e.g. FOIs, Subject Access Requests, ICO correspondence)
- Data breach reports
- Cyber security updates (provided by IT)

The Corporate Information Governance Group terms of reference can be viewed here.

4.1. Responsibilities

Strategic Leadership Team (SLT)
Overview
The Strategic Leadership Team (SLT) is made up of the Chief Executive and Directors of each Council directorate. Where required, Directors and/or Corporate Heads of Service may also attend as appropriate. The Data Protection Officer, Monitoring Officer and the Council's Senior Information Risk Owner (SIRO), provides a link between the CIGG and senior management

Formal senior information governance roles		
Staff name	**IG Role**	**Role**
Sue Cuerden	Senior Information Risk Owner (SIRO)	Executive Director of Corporate Services

Rhian Allen	Data Protection Officer (DPO)	Information Governance Manager

Document and version control	
Title of document	Information Security and Governance Policy and Framework
Author	Rhian Allen
Job title of Author	Data Protection Officer
Approved by	Corporate Information Governance Group
Publication date	
For use by	
Why issued	
Review date	

Version control details

Version No.	**Author / editor**	**Version date**	**Approved by**	**Approval date**	**Overview of changes**
V1.0	LBS	Jan 2016			Draft Policy from Sutton used as the basis for the RBK Policy
V2.0	Rhian Allen	December 2018			GDPR Compliance section added
V2.1	ISGB-Kingston and Sutton	March 2019			Board approved annual review
V3	Rhian Allen	June 2025	Corporate Information Governance Group	16th June 2025	Policy bought up to date