

# Information Security and Governance Policy and Framework

---

## Contents

### **Information governance policy**

[Summary](#)

[Why is this important?](#)

[Scope](#)

[Strategy](#)

[Key principles](#)

[Related policies](#)

[Legal and regulatory framework](#)

[Review and evaluation](#)

[Responsibilities](#)

[Training](#)

[Other organisations](#)

### **GDPR Compliance**

[Data Retention and Disposal](#)

[Data Breaches](#)

[Subject Access Request \(SAR\)](#)

[Legal Basis for Processing](#)

[Consent](#)

[Privacy Notice/Policy](#)

[Data Subject Rights](#)

### **Information security**

[Summary](#)

[Why is this important?](#)

[Scope](#)

[Key principles](#)

[Review and evaluation](#)

[Responsibilities](#)

[Training](#)

### **GDPR Compliance**

[Information security and governance framework](#)  
[Responsibilities](#)  
[Key policies](#)

**Appendix A:**

[Information Security Governance Board Terms of Reference](#)

## **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 (see section 3.2 below).

### **1.2. Why is this important?**

Information is a vital asset, in terms of supporting the efficient management of services and use of resources, as well as playing a key part in service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

Information governance sets out the way the Council handles information about customers and employees, in particular personal and sensitive information. It provides a framework comprising: compliance with the law, guidance from central government, the Department of Health (DH) and other partners, and year-on-year improvement plans.

It is important to ensure that we are compliant in all areas of policy including FOI and GDPR (General Data Protection Regulations) and well managed information is key.

This brings together all aspects of information and records management, including data protection, Freedom of Information, ICT and physical information security and data quality.

### **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 strategy sets out the Council's approach to provide a robust approach to information governance and the management of information. The key components underpinning it are:

**Information Security & Governance Policy and Framework**

- the Council's information security and governance policy and framework, which defines the Council's arrangements for information governance
- an ongoing action plan arising from a baseline assessment against the information governance; and standards set out in the NHS Data Security & Protection Toolkit

To ensure an information governance culture is developed across the Council:

- training and guidance is provided to all Council staff - to achieve this, a rolling training plan will be maintained by the Information Security and Governance Board
- performance on the NHS Data Security & Protection Toolkit is monitored and submitted to the Department of Health each year
- implementation of the NHS Data Security & Protection Toolkit is reviewed on a regular basis by the Council's internal auditors and may be audited in the future by an external auditing agency commissioned by Department of Health
- implementation of the Council's information governance strategy, policy and action plan, supported by annual reviews of each, ensures information is managed effectively

### **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**

To promote openness, the Council will:

- ensure non-confidential information about the Council's activities and its services is available to the public through a variety of media, in line with the Council's Transparency Code and the Freedom of Information Act
- undertake or commission annual assessments and audits of its policies and arrangements for openness
- ensure service users have ready access to information under the Subject Access Request procedure
- maintain clear procedures and arrangements for liaison with the press and media
- maintain clear procedures and arrangements for handling residents' queries

#### **1.5.2 Legal compliance**

To promote legal compliance, the Council will:

- regard all identifiable personal information relating to service users as confidential (except where national policy on accountability and openness require otherwise)

## **Information Security & Governance Policy and Framework**

- carry out or commission annual assessments and audits of its compliance with legal requirements
- establish and maintain policies to ensure compliance with the data protection laws, including the General Data Protection Regulation (GDPR), Human Rights Act and common law confidentiality
- establish and maintain agreements for the controlled and appropriate sharing of personal information with other agencies, in line with relevant legislation (eg Health and Social Care Act, Crime and Disorder Act, Children Act etc)

### **1.5.3 Information security**

To ensure the security of information is maintained, the Council will:

- establish and maintain policies for the effective and secure management of its information assets and resources
- undertake or commission annual assessments and audits of its information and ICT security arrangements
- promote effective confidentiality and security practice to its staff through policies, procedures and training
- establish and maintain incident reporting procedures, and monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

### **1.5.4 Quality assurance**

To promote quality assurance, the Council will:

- establish and maintain policies and procedures for information quality assurance and the effective management of records
- undertake or commission annual assessments and audits of its information quality and records management arrangements
- require managers to take ownership of, and seek to improve, the quality of information within their services
- ensure that, wherever possible, information quality is assured at the point of collection
- set data standards through clear and consistent definition of data items, in accordance with national standards
- promote information quality and effective records management through policies, procedures, user manuals and training

## **1.6. Related policies**

- [Records Management](#)
- [Using Systems and Data](#)
- [Information Classification and Marking](#)
- [Information Security Incident Reporting](#)
- [Information Security Risk Management Policy](#)
- [ICT Technical Standards and Security Principles](#)

- 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 also has to meet legal and regulatory standards on information security, including:

- General Data Protection Regulation (EU) 2016/679
- Freedom of Information Act 2000
- Local Government Act 1972
- Public Records Act 1958 (where not superseded by the Freedom of Information Act)
- Data Protection Act 2018 (and subsequent Special Information Notices) (Currently being removed)
- Human Rights Act 1998
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992)
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Re-use of Public Sector Information 2003 (EU Directive)
- Public Interest Disclosure Act 1998
- Prevention of Terrorism (Temporary Provisions) Act 1989 and Terrorism Act 2000
- Road Traffic Act 1988
- Regulations under Health and Safety at Work Act 1974
- Health and Social care legislation such as:
  - NHS Sexually transmitted disease regulations 2000
  - National Health Service Act 1977
  - Human Fertilisation and Embryology Act 1990
  - Abortion Regulations 1991
  - Health & Social Care Safety and Quality Act 2015 (Applicable to Adult Social care only)

In relation to many of the above requirements, effective information governance has been mandated by a number of regulations such as:

- Caldicott: Report, audit and improvement on the use of Personal Identifiable Data
- Third party Codes of Connection (including the Public Services Network and NHS)

### **1.8. Review and evaluation**

## **Information Security & Governance Policy and Framework**

The Information Security Governance Board (ISGB) is responsible for the maintenance and review of this policy. Legal responsibility remains with the organisation's Caldicott Guardians and Senior Information Responsible Officer (SIRO).

Reviews may also take place following:

- major policy breaches
- the identification of new threats or vulnerabilities
- significant organisational restructuring
- significant changes to the Council's technical infrastructure

Evaluation will be carried out via a number of means, including:

- completion of the annual NHS Information Governance Statement of Compliance
- accreditation for third party Codes of Connection (including the Public Services Network and NHS)
- internal/external audit programmes

Evaluation will be based on a number of criteria, including:

- number of reported policy breaches
- external assessment of organisational policy compliance
- staff awareness
- evidence of organisational commitment

## **1.9. Responsibilities**

Information governance responsibilities include:

### **Information governance coordination**

Detailed coordination of information governance activity is managed by the ISGB.

### **Ownership of information assets**

Each identified asset will have an appointed owner who is ultimately responsible for its governance. For systems, this is a senior figure in the relevant service area. System owners are responsible for determining system or area access policies, in conjunction with advice from the system management and information governance leads.

### **System management**

Each system should have an identified owner. The governance role of the system owner is to implement the system-related processes that govern:

- management of access to the system
- audit of user activity
- system data validation processes (input, internal and output)
- supplier support (where applicable)

### **SIRO and Caldicott Guardian role**

The SIRO and Caldicott Guardian roles have responsibility for establishing and maintaining procedures governing access to, and the use of, person-identifiable data held or processed within systems or networks which are the responsibility of the Council, and also the transfer

## **Information Security & Governance Policy and Framework**

of such data from the organisation to other bodies. The Caldicott Guardian also agrees local procedures and protocols to ensure consistency with any relevant central government requirements and guidance.

### **Information security management**

The Council's shared ICT Shared service are responsible for leading development of appropriate ICT security policies, ICT security management, promotion of good security practice and leading on ICT security audit activity and compliance with accreditation for the Public Services Network (PSN).

### **Document and records management**

The Council's shared ICT Shared service lead on the development and implementation of systems and practices which enable compliance with the requirements of the Public Records Act, the Freedom of Information Act, the Data Protection Act, General Data Protection Regulations and other records management codes of practice.

### **Physical security**

Responsibility for the physical security of the building lie with Facilities Management and individual service managers, supported by the Council's Facilities Management contractor, and users are responsible for physical security of the information they use.

### **Line management / HR governance**

Organisational line managers are responsible for ensuring that appropriate activities (training/user management) are made available to staff, and that compliance with information security and governance policies, as well as relevant system/acceptable use policies and procedures are promoted.

### **General staff**

As part of an employee's terms and conditions of employment (contract) there is an agreement to maintain confidentiality of information, in line with the Data Protection Act and General Data Protection Regulations and the Council's information security and governance policies. Temporary and casual staff and third parties are not covered by the same employment contract and are required to sign a confidentiality agreement prior to being given access to information.

### **1.10. 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 DPO, 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

### **1.11. Other organisations**

## **Information Security & Governance Policy and Framework**

The Council recognises that information is shared with other organisations for effective service provision. It has established appropriate links with ‘partner’ organisations to enable this.

Information is shared under an overarching information sharing protocol, where relevant, and will only be shared for a defined purpose (as required by the Data Protection Act). Where information needs to be shared for new requirements, Departments should develop their own information sharing protocols with partner organisations. Data Privacy Impact Assessments will be completed where data is to be shared and a consistent approach to data sharing agreements and protocols will be adopted.

## **2. Information security**

### **2.1. Summary**

All staff and other users of the Council’s ICT services and other services, have a duty to protect the systems, information and data that they use.

This policy explains the importance of information security, the role the Information Security Governance Board (ISGB) and senior staff have in ensuring Council employees understand how to protect Council information.

### **2.2 Why is this important?**

Information is vital to the efficient and effective operation of the Council, and must only be used for its intended purpose (ie in support of Council operations). The objectives of the information security policy are to:

- ensure the Council’s information assets are protected and remain available
- maintain the privacy and trust of our users by ensuring any information they provide is kept secure and used in compliance with relevant legislation, regulations and third party agreements
- ensure that where the Council shares information with other parties, it is protected against unauthorised disclosure and managed in compliance with this policy and any agreed information sharing agreements and/or protocols
- enable the Council to maintain accreditation with third party Codes of Connection, including the Public Services Network (PSN) and NHS Information Governance Toolkit
- ensure all breaches of information security, actual or suspected, are reported promptly, investigated thoroughly and appropriate action is taken to address the particular incident and to minimise the risk of similar incidents occurring

### **2.3 Scope**

This policy covers all of the following, including (but not limited to):

- permanent staff
- temporary staff
- councillors
- third parties accessing the Council’s information assets and ICT resources (including suppliers, partners, work-experience staff, students)

## **Information Security & Governance Policy and Framework**

## **2.4. Key Principles**

There are six key principles related to the Council's Information Security Policy:

- information
- confidentiality
- integrity
- availability
- authentication and access control
- auditing

### **2.4.1. Information**

Information is regarded as an important asset and so will be protected, with due consideration for all regulatory and legislative requirements, and for any data sharing agreements or protocols agreed between the Council and other parties.

### **2.4.2. Confidentiality**

Appropriate measures must be taken to ensure that the Council's proprietary, private and client information is accessible only to people who are authorised to have access.

### **2.4.3. Integrity**

The accuracy and completeness of the Council's information must be maintained, and changes or modifications affecting it must be authorised, controlled and validated through appropriate business process controls. Staff should refer to the Council's Data Quality Strategy when considering the integrity of information.

### **2.4.4. Availability**

Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the Council's information (and any systems critical to the ongoing activities of the Council) must be recoverable through the development, maintenance, implementation and testing of appropriate disaster recovery and business continuity plans.

### **2.4.5. Authentication and access control**

All people and systems seeking access to Council information or computer systems must be appropriately authorised to do so and use a system account assigned to them by the Council. The privilege to view or modify information, computer programs or the systems on which information is stored, will be restricted to those people whose job functions absolutely require it.

Where we grant access to customers or businesses, they can only access and view information about themselves, having first established their identity credentials.

### **2.4.6. Auditing**

User accounts and activity on each of the Council's computers, firewalls and networks must be recorded and maintained in compliance with all security, retention, legislation and regulatory requirements and be available for review as required.

## **Information Security & Governance Policy and Framework**

Security policies are maintained to support these objectives, together with processes and procedures that are published on 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 ISGB
- applicable controls to be audited at least once every three years
- internal audits to be carried out annually
- 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 Assistant Director of Digital and ICT is responsible for maintaining information security policies, which are reviewed annually by the ISGB.

### **Information governance coordination**

The ISGB 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 ISGB 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 role**

The Caldicott Guardian is responsible for ensuring the lawful and ethical processing of personal information, both within Council and when it is shared with other organisations. The Department of Health publication [The Caldicott Guardian Manual 2010](#) describes the responsibilities of the role in more detail.

### **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.

Each quarter IAOs must formally review the risks to the confidentiality, integrity and availability of their information assets and report these findings to the Information Security and Governance Board.

#### **Role of the information asset administrator (IAA)**

Information asset administrators are Officers supporting IAOs and the ISGB process, by ensuring collection of relevant material for the quarterly updates. Ensure ISGB agenda stays on team meetings and good and bad practises are fed back to them and then included in the quarterly report. Also support the IAOs to ensure risk registers are updated on a quarterly basis or when a big change to a Directorate occurs.

#### **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 ICT Service Desk and to the Risk and Assurance Team.

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.

#### **Privacy assessments**

All projects and changes to systems, applications or the use of information must be subject to a privacy assessment to ensure that the change will have no adverse impact on the protection for the Council's information assets.

#### **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 understand and adhere to the Council's information security policies.

#### **Information Security & Governance Policy and Framework**

## 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

We have a robust and effective data protection program in place which complies with existing law and abides by the data protection principles.

**3.1. Data Retention and Disposal** – The Retention and Disposal Schedules ensure that we meet the ‘data minimisation’ and ‘storage limitation’ principles and that personal information is stored, archived and destroyed compliantly and ethically.

**3.2. Data Breaches** – Our information security incident procedure ensures that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach. Our procedure is available to all employees on the intranet making them aware of the steps to follow.

**3.3. Subject Access Request (SAR)** – Our SAR procedure accommodates the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our procedure is available to all employees on the intranet making them aware of the steps to follow.

**3.4. Legal Basis for Processing** - Processing activities and identifying our legal basis for processing are regularly reviewed and updated ensuring that each basis is appropriate for the activity it relates to. Our records of our processing activities are maintained, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.

**3.5. Consent** - The GDPR sets a high standard for consent. Consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires individual (‘granular’) consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service. The GDPR gives a specific right to withdraw consent at any time. Our consent is documented in our Information Asset Register ensuring that our obligations under Article 7 of the GDPR are met.

**3.6. Privacy Notice/Policy** – we have revised our Privacy Notices to comply with the GDPR, ensuring that all individuals whose personal information we process are informed of why we need it, how it is used, what their rights are, and who the information is disclosed to.

## Information Security & Governance Policy and Framework

**3.7. Data Subject Rights** - We provide easy to access information via our internal and external website to ensure individuals can enforce their data protection rights. Individuals have the right to access any personal information that we process about them and to request information about:

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store personal data for
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

## 4. Information security and governance framework

The Information Security Governance Board (ISGB):

- agrees roles and responsibilities across the organisation
- plans and resources organisation-wide information governance initiatives (such as training)
- identifies and implements methodologies for areas such as risk assessment, quality measurement
- reviews security incidents and initiates resolution and learning
- assesses and implements governance controls for information
- leads and facilitates development of information governance as part of the infrastructure of the organisation

See [Appendix A](#) for Information Security Governance Board terms of reference.

### 4.1. Responsibilities

<b>Strategic Leadership Team (SLT)</b>
<b>Overview</b>
The Strategic Leadership Team (SLT) is made up of the Chief Executive and Directors of each Council directorate. Where required, Assistant Directors and/or Corporate Heads of Service may also attend as appropriate.

The Head of Corporate Governance and (Interim) Monitoring Officer, who is the Council's Senior Information Risk Owner (SIRO), provides a link between the ISGB and senior management

**IG Role**

The organisation's SIRO attends SLT meetings and can provide feedback on any information governance-related issues to the Council's Chief Executive and Directors .

**Attendees**

**Staff name**

**Role**

--	--

**Formal senior information governance roles**

**Staff name**

**IG role**

**Title**

--	--	--

**Information Security and Governance Board**

The Information Security and Governance Board (ISGB) is chaired by the Assistant Director, Digital and ICT who is also the Council's Senior Information Risk Owner (SIRO).

Each directorate within the Council has an Assistant Director that attends the board as an Information Security Champion for their respective directorate. There is also representation from HR, ICT and Audit.

The ISGB is managed by ICT support and the programme is led by recommendations made via the board, with key officers assigned to lead on individual projects.

The Head of Service in each directorate is the Information Asset Owner (IAO). Each directorate also has an Information Asset Administrator who coordinates the risk management process on behalf of the IAOs in their directorate.

**Attendees**

**ISGB role**

**Title**

--	--	--

Associated ISGB Members		

### Directorate management teams

Each directorate nominates an executive head who is the directorate champion responsible for attending the ISGB, providing cascade to the DMT and directorate updates to the ISGB. The executive heads who attend the DMT provide feedback to their management teams on any information governance-related issues.

All executive heads of service have been assigned the role of IAO for their respective service area. Information security risk management within each service area is coordinated by information asset administrators (IAAs) who are nominated by the directorate. IAAs are also responsible for overseeing the reporting and management of security incidents in their areas.

This will be reviewed with the Direction of Travel changes for the Council.

### 4.2. Key policies

Policy title	Policy purpose	Policy owner	Approved by	Approved date
<a href="#">Information Security and Governance Policy and Framework</a>	Define the Council's policy for information security and governance and the framework that supports this	Records Manager	ISGB	Jan 2017
<a href="#">Using Systems and Data Policy</a> *	Define the Council's policy for use of systems and data.	Joint Head of ICT	ISGB	Jan 2017
<a href="#">Information Classification and Marking Policy</a> *	Define the Council's policy for classification and marking of information assets.	Joint Head of ICT	ISGB	May 2016

<a href="#">Information Security Risk Management Policy</a> *	Defines how to secure information assets	Joint Head of ICT	ISGB	February 2017
<a href="#">ICT Technical Standards &amp; Security Principles</a>	Define technical security controls for the Council's ICT infrastructure.	Joint Head of ICT	ICT Board	January 2016
<a href="#">Third Party Access Policy and Procedure</a>	Define the policy for third party access to the Council's systems and ICT infrastructure.	Joint Head of ICT	ISGB	Sept 2016
<a href="#">Information Security Incident Reporting Policy</a> *	Define the policy and procedure to follow in reporting all data breaches	DPO	ISGB	May 2016
<a href="#">Social Media Policy</a>	Define the use by staff of Social Media in relations to their work	Head of Communications	ISGB	January 2016
<a href="#">Records Management Policy</a>	Define the Council's approach to records management	Records Manager	ISGB	January 2017

\* Key policies will be issued/rolled out to staff via NetConsent Policy Management Software.

## Appendix A: Information Security Governance Board Terms of Reference

These terms of reference commit the Information Security Governance Board to:

- maintain and continually review the responsibilities for information security and Council's management accountability arrangements for information security and governance
- coordinate the activities of staff with information security and governance responsibilities
- continue to implement and review the information security and governance policy and framework

### Information Security & Governance Policy and Framework

- ensure the communication, adherence and signed acknowledgement of the information security and governance policy and framework to and by all internal and external personnel authorised to handle Council information, assets and resources
- ensure the Council's requirements for information handling is communicated to all staff (including permanent, temporary and third parties with access to Council information, assets and resources)
- monitor the Council's information handling activities to ensure compliance with policy, law, regulatory requirements and other guidance
- continually review the organisation's information security and governance work programme
- formally review risks and approve risk mitigation, and to maintain the corporate Information Asset Register, and regularly review and approve the content of the register
- ensure that training made available by the Council is taken up by employees (permanent staff, temporary staff, third parties accessing the Council's ICT resources including suppliers, partners, work-experience staff, students) as necessary to support their role
- ensure staff have access to appropriate and up-to-date guidance on keeping personal information secure and on respecting the confidentiality of service users
- promote the need for all staff to actively report information security incidents
- maintain the information security incident log and provide a focal point for the discussion and/or resolution of all known information security incidents
- commit adequate resources to achieve the above

<b>Document and version control</b>	
<b>Title of document</b>	Information Security and Governance Policy and Framework
<b>Author</b>	ICT Shared Service/ ISGB
<b>Job title of Author</b>	
<b>Directorate</b>	Resources
<b>Approved by</b>	
<b>Publication date</b>	
<b>For use by</b>	
<b>Why issued</b>	
<b>Review date</b>	

**Information Security & Governance Policy and Framework**

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
V1.1	Rhian Allen	December 2018			GDPR Compliance section added