London Borough of Sutton

Information Security and Governance Policy and Framework

Note: Before reading this policy please ensure you are referring to the latest version, as published on the Council's intranet. Information about the document and version control is also contained within this document.

Document and version control	
Title of document	Information Security and Governance Policy and Framework
Author	Paul Garlick
Job title of Author	Flexible Admin, Business Support and Records Manager
Directorate	Resources
Approved by	Information and Security Governance Board
Publication date	January 2016
For use by	All staff
Why issued	Action - Corporate Policy
Review date	January 2018

Version control details					
Version No.	**Author / editor**	**Version date**	**Approved by**	**Approval date**	**Overview of changes**
V1.0	Paul Garlick	Jan 2016		14 Jan 2016	This Policy was formed to bring together the following documents: ● Information Governance Policy ● Information Governance Framework ● Information Security Policy
V2.0	Paul Garlick	April 2016			Updated Executive Head - Adult, Social Care and Safeguarding details
V3.0	Paul Garlick	July 2016			Updated membership details of the board
V4.0	Paul Garlick	January 2017	ISGB	12 Jan 17	Role of the information asset owner and IAA inserted Legal and regulatory framework updated

					Updated key policies
V4.1	Bradley Peyton	July 2017			Updated ISGB member details to reflect current arrangements.
V4.2	Bradley Peyton	December 2017			Added new IAA for Peoples Directorate (Children's)
V5.0	Bradley Peyton	January 2018	ISGB	15 January 2018	General updates and revisions
V5.1	Bradley Peyton	June 2018			Added reference to DPA 2018 and other minor changes.

Document contents:

1. Information governance policy
- 1.1. Summary
- 1.2. Why is this important?
- 1.3. Scope
- 1.4. Strategy
- 1.5. Key requirements
- 1.6. Related policies
- 1.7. Legal and regulatory framework
- 1.8. Review and evaluation
- 1.9. Responsibilities
- 1.10. Training
- 1.11. Other organisations

2. Information security
- 2.1. Summary
- 2.2 Why is this important?
- 2.3 Scope
- 2.4. Key requirements
- 2.5. Review and evaluation
- 2.6. Responsibilities
- 2.7. Training

3. Information security and governance framework
- 3.1. Responsibilities
- 3.2. 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 the efficient management of services and 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 comprised of the compliance with the law, guidance from central government, the Department of Health (DH) and other partners, and year-on-year improvement plans.

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

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:

- 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 Information Governance 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 Governance Security Board

- performance on the NHS Information Governance Toolkit is monitored and submitted to the Department of Health each year

- implementation of the NHS Information Governance 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 the 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 requirements

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 on the Council and its services are available to the public through a variety of media, in line with the Council's code of openness 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 requires otherwise)
- Establish a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing
- Carry out or commission annual assessments and audits of its compliance with legal requirements

- establish and maintain policies to ensure compliance with data protection laws including the General Data Protection Regulation (GDPR) (Regulation 2016/679), Human Rights Act 1998 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 (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act etc)
- Where appropriate pseudonymise and encrypt personal data

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 IT security arrangements
- promote effective confidentiality and security practice to its staff through policies, procedures and training
- establish and maintain incident reporting procedures, and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

1.5.4 Information 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

- HR policies relating to an individual's employment, role and responsibilities (i.e. 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:

- The General Data Protection Regulation (GDPR) (Regulation EU 2016/679)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Local Government Act 1972
- Public Records Act 1958 (where not superseded by the Freedom of Information Act)
- 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

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 roles**
  The SIRO and Caldicott Guardian roles have overall legal 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 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 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 Document and Records Manager's role leads on the development and implementation of systems and practices which enables compliance with the requirements of the Public Records Act, the Freedom of Information Act, the Data Protection Act, the GDPR and other records management codes of practice.

- **physical security**
  Responsibility for the physical security of the building lies with Facilities Management, individual service managers and users who are all 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 laws 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 asked 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 (e.g. 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 and accessible to all staff as an up-to-date resource for current information and guidelines

1.11. Other organisations

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 and the

GDPR). Where information needs to be shared for new requirements, projects should develop their own information sharing protocols with partner organisations.

2. Information security

2.1. Summary

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

This policy explains the importance of information security, and 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 (i.e. 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 the 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)

2.4. Key requirements

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.

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 the Council's 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.

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 Joint Head of ICT 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.

- **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 the 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)**
  IAOs are senior/responsible individuals involved in running the relevant business. At Sutton Council, the Assistant Director for each unit is the responsible IAO.

  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. IAOs lead and foster a culture that ensures information is valued, protected and used appropriately.

  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 (ISGB). All risks have to be RAG rated and actions have to be set out to deal with medium and high risks. The IAO is responsible for ensuring the registers are maintained and updated. They also ensure the necessary Privacy Impact Assessments are completed in instances where assets are shared with third parties and where new processing activities are proposed.

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

  IAAs are officers that support IAOs and the ISGB process by ensuring collection of relevant material for the quarterly updates. They ensure that the ISGB agenda is actively discussed at team meetings and good and bad practices are fed back to them and then included in the quarterly report. IAAs also support the IAOs to ensure risk registers are updated on a quarterly basis or when there is a significant business change.

- **Information asset**

  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 to the ISGB.

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. Additionally, under the GDPR there is a duty to report all high risk breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. In some instances, individuals affected by the breach must be informed. All security beaches will be recorded, regardless of whether they need to be notified to the ICO.

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

3. 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.

3.1. Responsibilities

Corporate Management Team (CMT)	
Overview	
The Corporate Management Team (CMT) is made up of the strategic directors of each Council directorate. Where required, the assistant directors of service for the various directorates also attend. The Strategic Director of Resources, 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 sits on the CMT and can provide feedback on any information governance-related issues to the Council's Chief Executive and strategic directors.	
Attendees	
Staff name	**Role**
Niall Bolger	Chief Executive
Gerald Almeroth	Strategic Director - Resources
TBC	Strategic Director - Peoples
Mary Morrissey	Strategic Director - EHR
Imran Choudhury	Director of Public Health
Jessica Crowe	Assistant Director, Chief Executives Directorate - Customers,

	Commissioning and Governance

Formal senior information governance roles		
Staff name	**IG role**	**Title**
Gerald Almeroth	SIRO/ Information Governance Lead	Strategic Director - Resources
Richard Nash	Caldicott Guardian - Peoples (Children's)	Acting Director, People Services Directorate (Children's Social Care and Safeguarding)
Nick Ireland	Caldicott Guardian - Peoples (Adults)	Acting Director, People Services Directorate (Adult Social Care and Safeguarding)
Imran Choudhury	Caldicott Guardian - Public Health	Director of Public Health

Information Security and Governance Board		
The Information Security and Governance Board (ISGB) is chaired by the Strategic Director of Resources 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 the Business Support Team and the programme is led by recommendations made via the board, with key officers assigned to lead on individual projects. All Assistant Directors in each directorate are Information Asset Owners (IAOs). Each directorate also has an Information Asset Administrator who coordinates the risk management process on behalf of the IAOs in their directorate.		
Attendees		
Staff name	**ISGB role**	**Title**
Gerald Almeroth	● SIRO ● Chair ISGB	Strategic Director - Resources
Mark Lumley	● Lead responsibility for ICT security	Joint Head of ICT (Sutton and Kingston)

Bradley Peyton	• Records Manager	Insurance and Records Manager
Marie Gadsden	• Corporate HR Lead	HR Manager (Sutton and Kingston)
Margaret Culleton	• Internal Audit	Head of Audit
Nick Ireland	• Caldicott Guardian • IAO • Information Security Directorate Champion	Acting Director, People Services Directorate (Adult Social Care and Safeguarding)
Richard Nash	• Caldicott Guardian • IAO • Information Security Directorate Champion	Acting Director, People Services Directorate (Children's Social Care and Safeguarding)
Imran Choudhury	• Caldicott Guardian • IAO • Information Security Directorate Champion	Director of Public Health
Julie Turner	• IAO • Information Security Directorate Champion	Assistant Director (Interim) Resources Directorate - Business Services
Warren Shadbolt	• IAO • Information Security Directorate Champion	Assistant Director Environment, Housing and Regeneration (Safer and Stronger Communities)
Jessica Crowe	• IAO • Information Security Directorate Champion	Assistant Director, Chief Executives Directorate - Customers, Commissioning and Governance
Associated ISGB Members		
Jonathan Williams	• Deputy Information Security Directorate Champion	Interim Assistant Director, People Services Directorate (Children's Social Care and Safeguarding)
Tanya Campbell	• Peoples (Adults) Data Protection Practitioner • IGSoC • IAA	Information Governance Officer, People Services
Nadine Wyatt	• IAA	Participation & QA Manager - People Services
Alex Penfold	• IAA	Senior Business Support Officer - Resources
Ariadne	• IAA	Procurement and Data Intelligence

Anderson		Apprentice - Chief Executive
Chris Lyons	● IAA	Performance And Information Manager, Environment, Housing and Regeneration
Barry Holland	● Deputy Caldicott Guardian Directorate Champion	Interim Strategic Support Service Manager, People Services
TBC	● FOI Manager	Customer Care and Improvement Manager
David Grasty	● ICT	Service Development Manager, ICT

Adult Social Services Information Governance Working Group	
The Adult Social Services Information Governance Working Group brings together key staff responsible for Information Governance compliance within the People Directorate. The group is chaired by the Deputy Caldicott Guardian for People's (Adults) and meets regularly throughout the year to discuss information governance issues and complete relevant work streams aligned to the Information Governance Statement of Compliance.	
Attendees	
Staff name	**Role**
Barry Holland	Chair
Tanya Campbell	Information Governance Officer
Mark Horwood	Technical and Business Support Officer
Margaret Culleton	Head of Audit
Bradley Peyton	Records Manager
Mark Lumley	Joint Head of ICT (Sutton and Kingston) [where required]

Directorate management teams

All directorate management teams (DMTs) meet monthly, where information governance is an agenda item for discussion and update.

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

All Assistant Directors 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.

3.2. Key policies

Policy title	Policy purpose	Policy owner	Approved by	Approved date
Information Security and Governance Policy and Framework	Define the Council's policy for information security and governance and the framework that supports this	Records Manager	ISGB	January 2018
Using Systems and Data Policy *	Define the Council's policy for use of systems and data.	Joint Head of ICT	ISGB	January 2017
Information Classification and Marking Policy *	Define the Council's policy for classification and marking of information assets.	Joint Head of ICT	ISGB	May 2016
Information Security Risk Management Policy *	Defines how to secure information assets	Joint Head of ICT	ISGB	February 2017
ICT Technical Standards & Security Principles	Define technical security controls for the Council's ICT infrastructure.	Joint Head of ICT	ICT Board	January 2016
Third Party Access Policy and Procedure	Define the policy for third party access to the Council's systems and ICT infrastructure.	Joint Head of ICT	ISGB	Sept 2016
Information Security Incident Reporting Policy *	Define the policy and procedure to follow in reporting all data breaches	Records Manager	ISGB	October 2017
Social Media Policy *	Define the use by staff of Social Media in relations to their work	Head of Communications	ISGB	January 2016
Records Management Policy *	Define the Council's approach to records management	Records Manager	ISGB	January 2018

* 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 the 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

- 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 the Council's 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