POLICY & RESOURCES COMMITTEE	Agenda Item 129 Brighton & Hove City Council

Subject:		**Information Governance Strategy**		
Date of Meeting:		**11 February 2016** 12 January 2016 – Audit & Standards Committee		
Report of:		**Head of Law and Monitoring Officer**		
Contact Officer:	**Name:**	**Abraham Ghebre-Ghiorghis** **Anita Baxter**	**Tel:** **Tel:**	**291500** **295095**
	Email:	**abraham.ghebre-ghiorghis@brighton-hove.gov.uk** **anita.baxter@brighton-hove.gov.uk**		
Ward(s) affected:		**All**		

FOR GENERAL RELEASE.

1. PURPOSE OF REPORT AND POLICY CONTEXT

1.1 The purpose of this report is to seek comments from the Committee on the draft Information Governance Strategy (attached as an Appendix) before consideration and approval of the strategy by the Policy & Resources Committee.

2. RECOMMENDATIONS:

2.1 That Members consider the attached draft Information Governance Strategy 2016-19 (appendix 1) and comment as necessary.

2.2 Note that any comments will be incorporated into a revised draft going to the Policy & Resources Committee for final approval.

3. CONTEXT/ BACKGROUND INFORMATION

3.1 Information governance has over the last few years grown in importance to reflect public expectation and complex laws that govern data protection, access to information and proper management of records. This trend has been accentuated with the increasing digitalisation of services and the way people prefer to access services.

3.2 The attached draft Information Governance Strategy has been developed by the Information Governance Team and agreed by the Information Governance Board which is chaired by the Chief Executive and has representatives from key Council directorates. It sets out Information Governance aims and deliverables over the next 4 years.

3.3 Some key aims of the strategy include:

- Ensuring that information governance policies are embedded in the day to day operations of the organisation;

- Ensuring a high level of staff and supplier awareness through education and fostering a culture of personal responsibility, ownership and commitment to high standards
- Ensuring that there are proper audit and assurance processes to check whether information governance polices are being implemented
- Implementing a comprehensive information security management system (ISMS) aligned to international best practice standards ISO 270001.
- Ensure safe and proper records and information management.

3.4. A high level of deliverables or actions to support the achievement of the aims is set out in section 7 of the strategy (see appendix 1)

3.5. Section 8 of the report sets out the information governance framework roles and responsibilities. More detailed information with terms of reference is attached in Appendix 2. This includes the roles of the Information Governance Board, the Senior Information Risk Owner, the two Caldicott Guardians, the Information Management Team and the Information Asset Owners.

3.6. The adoption of the strategy will help the Council achieve better levels of compliance with the law and best practice.

3.7 The strategy needs to be approved by the Policy & Resources Committee, but given its role in assuring proper governance, including information governance, it has been referred to this committee for information and comment. Any comments received will be incorporated in the final draft going to the Policy & Resources Committee.

4. ANALYSIS & CONSIDERATION OF ANY ALTERNATIVE OPTIONS

4.1 The adoption of the strategy will help the council comply with regulatory and good practice requirements.

5. COMMUNITY ENGAGEMENT & CONSULTATION

5.1 Relevant staff were consulted and the draft was approved by the Information Governance Board.

6. CONCLUSION

6.1 That the strategy be agreed subject to any comments or suggestions from the committee

7. FINANCIAL & OTHER IMPLICATIONS:

Financial Implications:

7.1 The costs of reviewing the Information Governance Strategy will be met within existing council resources.

Finance Officer Consulted: Peter Francis *Date: 04//01/16/*

Legal Implications:

7.2 The adoption of the strategy will assist the Council in complying with its legal obligations regarding data protection, freedom of information, human rights law and requirements of regulatory bodies,

Lawyer Consulted: Abraham Ghebre-Ghiorghis *Date: 29/12/2015*

Equalities Implications:

7.3 None arising from the report

Sustainability Implications:

7.4 None arising from the report

Any Other Significant Implications:

7.5 None

SUPPORTING DOCUMENTATION

Appendices:

1. Information Governance Strategy
2. Information Management Frame work-roles and responsibilities

Documents in Members' Rooms

None

Background Documents

None

Appendix 1

Brighton and Hove City Council

Information Governance Strategy 2016-19

Contents

1.0 Executive summary

This strategy describes Brighton and Hove City Council's information governance aims and deliverables over the next three years.

It asserts the council's commitment to compliance with information rights legislation, robust records management and compliance with HMG and other security requirements. It also confirms our commitment to good practice through the implementation of, and adherence to, a comprehensive suite of policies and guidance.

It sets out an approach that actively enables and supports the delivery of corporate objectives and exploits opportunities for business benefits whilst delivering the requirements of the various compliance regimes. It is an approach that aims to be flexible and responsive to new or changed operational requirements, and that establishes the capacity of the

organisation to take proportionate risk in accordance with a defined risk appetite.

The strategy establishes a framework for creating effective information governance that helps us to make the best use of our information assets and as a consequence support the delivery of our corporate objectives and the improvement of our business processes.

This approach will further the Council's aim 'to provide open civic leadership and effective public services' through being transparent, open, and accountable about what we do and for the actions we take.

It will support the confidence of our citizens that their personal information will be managed in accordance with their rights.

The Information Governance team will set out and communicate our information governance strategy and champion the information governance agenda. The team will engage with business areas across the organisation to ensure that the corporate information governance policy framework is understood widely and is properly aligned with business and operational requirements. The team will work with, and provide specialist advice and support to:

- Citizens
- Executive Leadership Team
- Senior Information Risk Owner
- Information Asset Owners (IAO)
- Staff
- Partners
- Suppliers

2.0 Introduction

This strategy covers the period March 2016 - Dec 2019 and sets out the on-going development, implementation and embedding of a robust information governance framework for the effective management and protection of BHCC's information assets.

Information governance is the discipline within which accountability, standards, policies and procedures are developed and implemented. Good information governance practices aim to ensure that all information created, obtained or received, by BHCC is managed, accessed, used and disposed of appropriately. Effective Information Governance ensures that information assets are compliant with our regulatory obligations, support the rights of our citizens and are cost effective.

BHCC has a responsibility to manage and protect a wide range of information to ensure that it remains confidential and preserves its integrity and availability. Information types include:

- personal and sometimes sensitive information provided by citizens relating to provision of services
- information about our services and how they are provided
- information which supports the running of our organisation including records relating to staff and our IT
- information about the strategies and policies of our organisation

3.0 BHCC Corporate Plan 2015 -19

In the Corporate Plan 2015-19 BHCC describes two of its four objectives as building an organisation that is publicly accountable and citizen focused. This is in the context of significantly reduced budget and growing demand. If we are to achieve these objectives we must create an environment in which citizens and other agencies with which we work trust us to look after their information responsibly, securely and fairly.

To achieve this we must ensure that;

- our staff have a high level of awareness of all their obligations under information rights law and other regulatory requirements, and that those obligations are routinely met in practice
- that good information handling practice is embedded into the culture and day to day business processes of the organisation and into the design and acquisition of new technologies and systems
- our information management processes are streamlined, cost effective and robust, creating a high level of confidence in the quality of our information that supports efficient day to day practice and good decision making. Furthermore, this is essential to the secure exchange of information with other agencies with which we must collaborate to deliver more shared services.

This information governance strategy is a clear statement of BHCC's commitment to high quality information management and to technical and physical information security good practice. It recognises that investment in

information governance supports and contributes to both our corporate objectives and our regulatory responsibilities

The strategy also establishes our commitment to ensuring effective information governance practice as a means to enable our organisation to operate openly and efficiently in an increasingly digital environment.

4.0 Regulatory environment

BHCC is a data controller and as such is subject to a regulatory framework, including but not limited to:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003

Other related legislation:

- The Public Records Act 1958
- The Re-use of Public sector Information Regulations 2005
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Local Government Acts
- Copyright Design and Patents Act
- Common Law – duty of confidentiality

Related guidance and codes of good practice:

- Security Policy Framework (Cabinet Office).
- Public Service Network (PSN) Code of Connection.
- The Health and Social Care Information Centre, Information Governance Toolkit
- Information Commissioner's Office guidance and standards
- ISO 27001: 2013 – Information Security Management Systems
- ISO 15489:1&2 – The International Standard for Records Management
- e-Government Metadata Standard version 3.1
- The Lord Chancellor's Code of Practice on Records Management

5.0 Scope

This strategy is applicable to all BHCC staff and all departments, sections, services, information systems and records and other information assets of the Council and includes within its scope;

- The framework of accountability and responsibility for information assets
- The processes by which information is created, accessed and used
- The arrangements under which the Council uses the information of its partners and/or allows its partners to use its information.
- The efforts to build high quality information practice in staff and partners through education and awareness

6.0 Information governance aims

There are three elements to the BHCC information governance landscape; information security, data protection and records management. Each element requires policy, process and defined standards. There are overlaps between the three elements but each has as its primary focus and together they form a complete information governance discipline. BHCC's information governance aims are described below and encompass all three elements. Achievement of these aims will deliver essential compliance requirements but will also enable and support our business and deliver business benefits.

The high level deliverables to support the achievement of these aims are described in section 7.0 below.

6.1 Policy

We will ensure that our information governance policies are embedded in the day to day operations of the organisation, that they are compliant with relevant legislation, standards and codes of practice, demonstrate good practice and meet the public interest.

The policies are based on a risk management approach that recognises that information has significant value, are commensurate with our stated risk appetite and are aligned with business requirements.

6.2 Education and Awareness

We will aim to embed a high level of staff and supplier awareness of information governance policy and process to help achieve compliance and reduce the risk of avoidable incidents and breaches through human error.

We will foster a culture of personal responsibility, ownership and commitment to high standards in information handling to support and enable our business processes.

6.3 Audit and assurance

We will ensure that there are processes in place to check whether information governance policy is being implemented and measure the effectiveness of the control environment.

We will work with business areas and Information Asset Owners to gain feedback about the practical operation of policy. We will act on this feedback and make changes where necessary.

The Information Governance team and IAOs will work together to share experience and maximise the opportunities to learn from examples of good practice, both internal and external.

6.4 Records and information management

We will ensure that staff competency in records management is developed and supported by appropriate technologies and processes, so as to achieve the following benefits:

- Information is trusted, authentic and reliable
- Information enables high quality decision making
- Information quality contributes to improved public confidence in the council
- Information supports effective and timely services for vulnerable citizens
- Information handling is efficient and cost effective
- Information supports and does not hinder internal/external collaboration

6.5 Information security

We will implement a comprehensive information security management system (ISMS) aligned to the international best practice standard ISO 270001. This will ensure that the council has robust, proportionate, cost effective and compliant information security measures in place so that that the organisation is protected against threats from unauthorised or unintended access, destruction, disclosure and tampering.

We will work with business areas to ensure that information security policy is aligned with operational requirements and find solutions appropriate to BHCC’s risk appetite. We will support our people by ensuring that information security policy and processes are clear and easy to

understand, that help and guidance are available when needed, and by providing appropriate training to minimise the risk of human error.

We will provide an assurance function (Information Security Team) that sets clear security standards against which all technology developments are measured.

6.6 Collection and use of personal information

The Data Protection Act 1998 sets out the requirements and safeguards which must be applied to personal data to ensure the rights and freedoms of living individuals are not compromised. It is BHCC's obligation as Data Controller to comply with the Act.

We will:

- Comply with the law in respect of the data we hold about individuals
- Hold information securely and confidentially
- Obtain information fairly and efficiently
- Record information accurately and reliably
- Share information appropriately and lawfully

In addition we will promote transparency and openness about how we handle personal information providing confidence to the individuals and third parties who pass personal information to us.

7.0 Deliverables

The high level deliverables to support the achievement of the BHCC's information governance aims are outlined in the tables below.

7.1 Policy

	Compliance	Business benefits
Develop and review all information governance policies and process	Ensures policy set is complete and up to date. Policies must achieve legal and regulatory compliance and demonstrate good practice	Policy is aligned with business practice and operational requirements Staff know what to do
Provide accessible underpinning guidance in a range of formats to support policy	Improves compliance and helps reduce avoidable human error.	Ease of access leads to better compliance and efficiency

7.2 Awareness

	Compliance	Business benefits
Annually review and	A well informed workforce	Awareness programme is

update education, awareness and training programme for all staff	reduces the risk of information incidents and facilitates compliance with the legal framework	tailored to job roles and business processes. One size does not fit all A raised level of awareness of information governance embeds good practice, creates efficiencies and delivers improved services to the public Skills are transferrable across services and roles

7.3 Audit & Assurance

	Compliance	Business benefits
Implement a risk management framework	A coherent and organisation wide approach to the identification, assessment and treatment of risk which aligns to the requirements laid down by our compliance regimes and best practise.	Aides with the protection and preservation of Confidentiality, Integrity & Availability (CIA) of information assets. This reduces the risk of loss of IT services critical to the operation of the business and lowers the likelihood of reputational and financial damage. Develops a risk appetite that allows for proportionate risk taking. Empowers people to act appropriately
Provide an advice and assurance function, supported by robust documentation across all three domains (Infosec, DP and RM).	Demonstrates adherence to our own standards and policies.	Enables the business to seek and obtain appropriate advice and allows reliance on the controls and measures in place.
Monitor compliance through the independent internal audit function.	Appropriate technical and organisational measures are in place.	Identifies gross risks to allow the smooth delivery of services.
At least annual penetration testing.	Required by our compliance regimes and provides external & independent assurance over our technical security.	Protects the CIA of information assets.

Review and develop management information and key performance indicators that are accurate and fit for purpose and produce improvement plans	Supports compliance with the legal and regulatory framework	Supports business to make informed decisions.

7.4 Records and information management

	Compliance	Business benefits
Design and implement a framework for appropriate management of the Council's records. This includes: • Corporate Retention Schedule • Business Classification Scheme • Records Management Architecture • Digital Records Toolbox • ECM and Digital Consultancy Service • Information Asset Register • Records Training and Awareness initiatives	A consistent approach to creating, storing, maintaining and disposing of records and data improves ability to comply with public information rights and contributes to ensuring that information is used in the public interest. Accountability for records assets is maintained at appropriate levels of the organisation	Authentic and credible information is more easily found and used. Decision making is enhanced by higher quality evidence Records related risk is managed Records are retained in a usable form for as long as required to meet the Council's interests and obligations. Information management is cheaper

7.5 Information Security

	Compliance	Business benefits
Set the standards to enable compliance with IS0 27001, HSCIC IG Toolkit, PSNA Code of Connection and other security standards as appropriate	Achieves compliance with the regulatory framework Business information is protected against threats from unauthorised or unintended access, destruction, disclosure and tampering.	IT services are available and business is not interrupted Essential to the development of shared and collaborative services with other agencies
Document and implement a suite of user and technical information	Achieves compliance with regulatory framework	Normalises expected standards and supports efficient business

security procedures		practices

7.6 Collection and use of personal information

	Compliance	Business benefits
Put in place and develop appropriate measures to ensure best practice in handling of personal information; For example; • Information Sharing Protocols • Privacy Impact Assessments • Privacy notices • Data Processing Agreements	Achieves compliance with the legal and regulatory framework	Gives confidence to citizens, partners and staff that we are sharing data appropriately. Embeds efficient information handling practice Allows for data to be used across services & improves efficiency and cost effectiveness.

8.0 Information governance management framework - roles and responsibilities

We will have appropriate structures in place to ensure that there are clear delegated duties, responsibilities, decision-making powers and processes embedded within BHCC's operational processes. Roles and responsibilities are described in brief below.

8.1 The Information Governance Board (IGB)

The IGB is the executive level board that champions IG across the organisation and provides advice and support to the SIRO. It is chaired by the Chief Executive.

8.2 Senior Information Risk Owner (SIRO)

The SIRO is a member of BHCC's Executive Leadership Team.
Their role is to take ownership of the organisation's information risk policy, act as an advocate for the management of information risk on the Executive Leadership Team and provide written advice to the Audit and Standards Committee through the annual governance statement in regard to information risk.

The SIRO has overall responsibility for understanding how the strategic business goals of the organisation may be impacted by information risk and for sponsoring and promoting information governance policy across the organisation.

8.3 Caldicott Guardian

The Caldicott Guardian plays a key role in ensuring that BHCC and partner organisations satisfy the highest practical standards for handling patient/service user-identifiable information. They acting as the ‘conscience’ of an organisation.

The Caldicott Guardian also has a strategic role alongside the SIRO to champion information governance requirements and issues at Board / senior management level and, where appropriate, at a range of levels within the organisation’s overall governance framework.

8.4 The Information Governance Team

The Information Governance team is responsible for the provision of subject matter expertise to the organisation within the disciplines of Information Security, Information Rights and Records/Content Management. It supports compliance with relevant legislation, compliance standards and best practice.

8.5 Information Asset Owners (IAO's)
IAOs are accountable for the quality of and access to information created, received or obtained by their business area. Additionally IAOs are responsible for identifying, assessing and managing the risk associated with their information assets.

8.6 BHCC's staff
All BHCC staff have a personal responsibility to understand and comply with the information governance policies and any procedures applicable to their specific role.

8.7 Independent Assurance
BHCC will have in place external independent assurance arrangements to ensure compliance with information governance and information security legislation, regulations and good practice.

8.8 Information Governance Working Groups
We will establish appropriate IG working groups in specific subject matter areas to champion IG matters. For example;

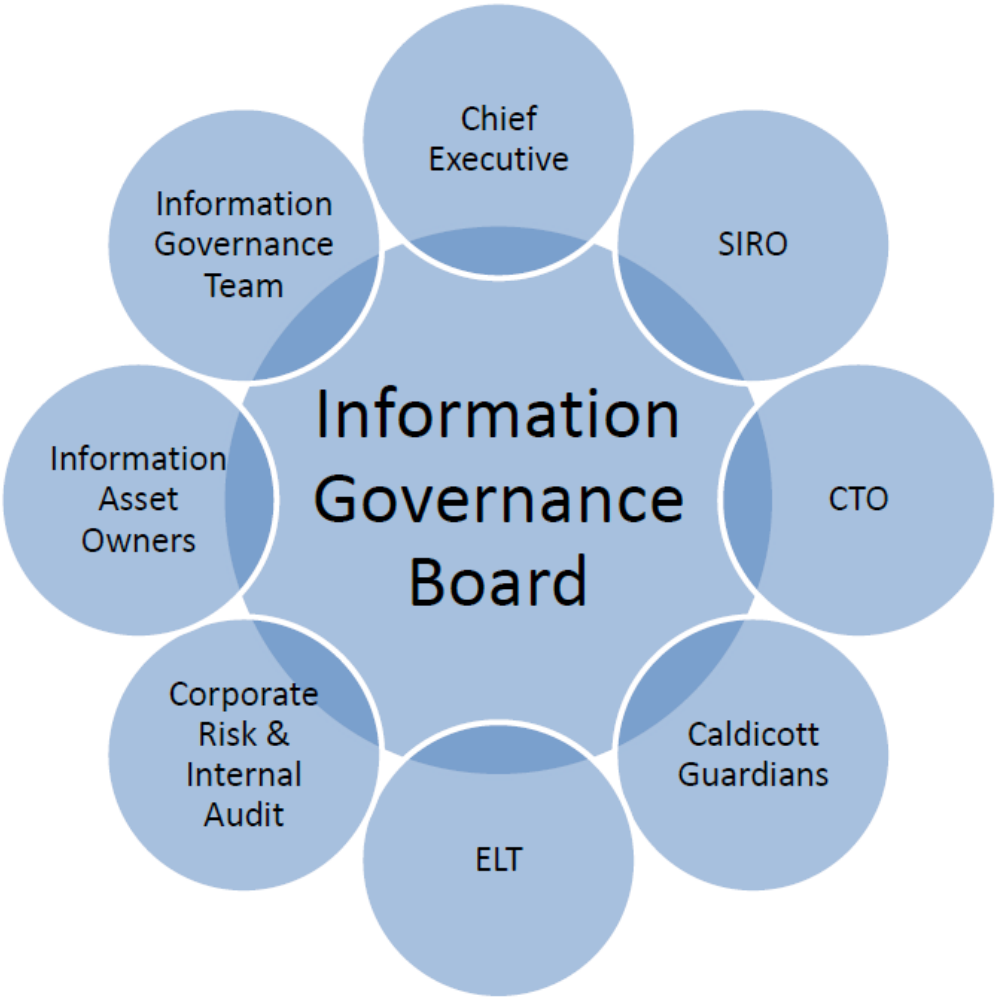
- a security working group whose role is to contribute to the understanding, identification, and control of information security risks in line with BHCC's information risk appetite

- a physical security working group in which the Facilities Team and the Information Security team work together to ensure that the physical security arrangements in BHCC sites are commensurate with the relevant standards.

- an IAO working group that develops the role and competencies of the IAOs and ensures there is a forum to raise concerns and share experience. Developing into a 'community of practice'.

Appendix 2

Information Governance at BHCC



Information Governance Board (IGB)

Terms of Reference

Members

Chief Executive Officer, Chair
Senior Information Risk Owner ('SIRO')
Chief Finance Officer
Caldicott Guardian/s
Chief Technology Officer
Head of Audit
Head of Human Resources and Organisational Development
Corporate Risk Management Lead
Information Asset Owner

Advisors

Head of ICT Business & Governance
Data Protection Manager
Information Security Manager
Records Manager

Purpose

The Information Governance Board will provide leadership in information governance good practice to ensure that the *value* of our core business information is protected and enhanced. This will guard against harmful threats and vulnerabilities, reduce cost and support our ambition to collaborate and share information to improve services to citizens. The Board will set the standards for information governance, ensure that these standards are embedded within the organisation, communicate key messages to the organisation.

The IGB is an advisory body with responsibility for co-ordinating policy and practice across the organisation and ensuring compliance with the law, government guidance and general good practice.

Formal decision-making power in relation to information governance and operational policies is delegated by Policy and Resources Committee to the Executive Director, Finance and Resources. Members of the Board can also use their own delegated powers to take steps or implement proposals in their directorates.

Responsibilities

The Information Governance Board will:

- Advise ELT of key information governance issues

- Agree information governance policy and standards and recommend formal approval to the Executive Director of Finance & Resources or the Policy & Resources Committee where necessary
- Monitor implementation of the Information Governance Strategy challenge performance and provide leadership where conflicts occur
- Provide corporate governance, assurance and risk ownership for information governance
- Receive and review reports into breaches of confidentiality and security and ensure remedial action is effectively communicated and implemented
- Communicate key messages to the organisation

Frequency

The IGB will meet bi-monthly.

Review cycle

This document will be reviewed annually or wherever there may be a change of influencing circumstances.

Approval Date – 15th December 2015

Senior Information Risk Owner

Role

The Senior Information Risk Owner (SIRO) has overall responsibility for understanding how the strategic business goals of the organisation may be impacted by information risks. He or she is a member of the Executive Leadership Team (ELT) and a member of the Information Governance Board (IGB). The seniority of the role in the organisation is a key factor in ensuring the appropriate management of information.

Key SIRO responsibilities

- ensures that the Council's approach to information governance risk is effective in terms of resource, commitment and that it is communicated to all staff
- responsible for describing, defining and reviewing the corporate risk appetite for information risk
- takes ownership of the information risk management approach and provides a focal point for managing information risks and incidents
- makes decisions in respect of the reporting of incidents to the Information Commissioner's Office
- is accountable for information governance processes
- fosters a culture for protecting and using information
- is concerned with the management of information assets
- ensures that ELT and the appropriate committee are regularly briefed on information governance and risk

Other Key Information Governance Roles in relation to the SIRO

Senior Information Risk Owner (SIRO)	Is accountable for the management of risk in respect of all information held by the organisation. He or she operates at an executive level and receives assurances that all relevant Information Governance Processes, procedures and policies are in place.
Caldicott Guardians (Children's Services and Adult Social Care)	Is concerned with the management of patient/service user information. He or she operates at an executive level. The role is advisory, and accountable for that advice. The Caldicott Guardian is the conscience of the organisation and provides a focal point for patient/service user confidentiality & information sharing issues.
Information Governance Board (IGB)	Provides advice and assurance to SIRO in respect of IG requirements, risks and incidents.
Information Asset Owners (IAO's)	IAO's are senior individuals responsible for managing risk in respect of the information assets that they "own". IAO's are responsible for providing assurances to the SIRO though the delegated

	framework.
Information Security Manger	Provides expert advice to SIRO, Caldicott Guardian, IGB and staff.
Data Protection Manager	Provides expert advice to SIRO, Caldicott Guardian, IGB and staff.
Records Manager	Provides expert advice to SIRO, Caldicott Guardian, IGB and staff.

BHCC Caldicott Guardian

Role

The Caldicott Guardian plays a key role in ensuring that BHCC and partner organisations satisfy the highest practical standards for handling patient/service user-identifiable information. Acting as the 'conscience' of an organisation, the Guardian should also actively support work to facilitate and enable information sharing, and advise on options for lawful and ethical processing of information as required. Local issues will inevitably arise for Caldicott Guardians to resolve. Many of these will relate to the legal and ethical decisions required to ensure appropriate information sharing. It is essential in these circumstances for Guardians to know when, and where, to seek advice.

The Caldicott Guardian also has a strategic role alongside the SIRO to champion information governance requirements and issues at Board / senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework.

Key Caldicott Responsibilities

- the Caldicott Guardian sits on organisation's Information Governance Board and acts as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.

- the Caldicott Guardian champions confidentiality issues at Board/senior management team level and develops their knowledge of confidentiality and data protection matters, drawing upon internal and external expertise where appropriate.

- the Caldicott Guardian ensures that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key areas of work that need to be addressed by the organisation's Caldicott function are detailed in the Information Governance Toolkit.

- the Caldicott Guardian should oversees all arrangements, protocols and procedures where confidential patient / service user information may be shared internally and with external bodies.

The relationship with the Senior Information Risk Owner

There are a number of differences between the roles of the Caldicott Guardian and the SIRO that suggest that they should normally remain distinct and separate; for example, the Caldicott Guardian's main focus is patient identifiable information whereas the SIRO is concerned with the risks to information generally. At the same time there is clearly a need to ensure that the Caldicott Guardian works closely with the SIRO (and any organisational Information Asset Owners – IAOs) and that the Guardian is consulted where appropriate when information risk reviews are conducted for assets which comprise or contain patient/service user information. The Caldicott Guardian should 'sign-off' information risk reviews in these circumstances.

Information Asset Owner

Role

Information Asset Owners (IAO's) are senior individuals responsible for the running of the relevant service; in BHCC this is usually a Head of Service. Their role is to understand what information is held by their business area, what is added and what is removed, how information is moved, and who has access to it 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.

Key IAO responsibilities

- Leads and foster a culture that values, protects and uses information for the public good
- Knows what information the asset holds, and what enters and leaves it and why
- Knows who has access and why, and ensures their use of it is monitored
- Understands and addresses risks to the asset, and provides assurance to the SIRO
- Responsible for ensuring that Information Rights access requests (including SARs, FOIs, EIRs, Section 29, etc)re fulfilled in accordance with statute
- Ensures the asset is fully used for the public good