University of Oxford

Cancer Epidemiology Unit (CEU)
Information Governance Policy

Version 1.0

Version History

Version	Issue Date	Author	Description
1.0	June 2014	Lucy Wright	Initial version

Table of Contents

1 Distribution and approval

This is a controlled document with read-only rights for unit staff and administrative rights for the Information Governance Lead.

Title:	CEU Information Governance Policy
Location:	v:/IG_policies
Owner:	Information Governance Lead
Approver:	Unit Management Committee [Note: Updates may be made to the appendices to correct or update matters of fact. Changes to the main document or to the Terms of Reference for the Information Governance Committee require formal approval.]
Review:	At least annually (and more frequently if required to make improvements in response to experience, audits or incident management findings)
Applicability:	All information activities conducted by or on behalf of the Unit.
Interpretation:	Questions relating to the interpretation of this policy should be directed initially to the Information Governance Lead
Unit:	Cancer Epidemiology Unit (CEU) within the Nuffield Department of Population Health, University of Oxford

2 Abbreviations and definitions

Abbreviation	Description
Information Governance Toolkit	The Information Governance Toolkit is a performance tool produced by the Department of Health and hosted by the Health and Social Care Information Centre (HSCIC). It draws together the legal rules and central guidance set out above and presents them in one place as a set of information governance requirements. The Unit is required to carry out self-assessments of their compliance against the IG requirements. https://www.igt.hscic.gov.uk/about.aspx?tk=416994034578820&cb=09%3a46%3a08&clnav=YES&lnv=5

Abbreviation	Description
Information Assets	Information Assets are identifiable and definable assets owned or contracted by the Unit and which are 'valuable' to the business of the Unit. Information Assets may include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data, though Information Assets should not be seen as simply technical. There are many categories of Information Assets including: • Information: databases, system documents and procedures, archive media/data, paper records etc. • Software: application programs, system, development tools and utilities. • Physical: infrastructure, equipment, furniture and accommodation used for data processing. • Services: computing and communications, heating, lighting, power, air-conditioning used for data processing. • People: their qualifications, skills and experience in use of information systems. • Intangibles: For example, public confidence in the organisation's ability to ensure the confidentiality, integrity and availability of personal data. As these categories suggest, Information Assets are not necessarily tangible objects; business processes and activities, applications and data should all be considered as Information Assets. However, their degree of importance to the organisation may vary.
IT	Information Technology
Personal data	Personal data means data which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. (http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#personal-data)
Sensitive personal data	Sensitive personal data means personal data consisting of information as to: (a) the racial or ethnic origin of the data subject, (b) his/her political opinions, (c) his/her religious beliefs or other beliefs of a similar nature, (d) whether his/her he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his/her physical or mental health or condition, (f) his/her sexual life, (g) the commission or alleged commission by him/her of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings. http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions#personal-data
SIRO	Senior Information Risk Owner (see section 6.2.4)
Unit	The research unit within the Nuffield Department of Population Health to which this policy applies (see Appendix I)

Abbreviation	Description
Unit Management	The person or committee responsible for senior leadership of the Unit (see Appendix I)
University	University of Oxford

3 Introduction

3.1 Information Governance

Information Governance encompasses the way organisations 'process' or handle information. It covers personal information (i.e. that relating to patients/service users and employees), and corporate information (e.g. financial and accounting records, scientific data and results). Information Governance provides a way for employees to deal consistently with the many different rules about how information is handled.

This policy defines the framework for robust Information Governance (including Information Security) within the Unit. This policy is the primary policy for this activity, beneath which reside a number of other technical and security related policies (see Appendix II).

3.2 Strategic aims

The Unit's information systems and the data they contain underpin all of the Unit's research, teaching and operational activities, and are essential to the Unit's goal to produce reliable research evidence and effectively train and develop students and staff to be able to conduct such research. The Unit recognises the need for staff, students and collaborating clinicians and academics to have access to the information they require in order to carry out these activities. Information Governance and Security must therefore be an integral part of the Unit's management structure in order to meet the following objectives:

- protect the rights and well-being of research participants and staff;
- generate reliable research results;
- maintain trust in the Unit, the University and the wider academic and clinical communities; and
- comply with University regulations and policies, and with legal, regulatory and other external obligations (e.g. from funders).

3.3 Implementation

There are two key components underpinning the Unit's Information Governance strategy:

- this Unit **Information Governance Policy**, which outlines the principles, responsibilities and management of Information Governance within the Unit; and
- an annual **Information Governance Improvement Plan** arising from assessment against this Policy and other external standards such as those set out in the NHS Information Governance Toolkit.

The Unit will ensure that this Information Governance Strategy is implemented through detailed policies and procedures, training and awareness, and that appropriate resources are provided to support these activities.

The Unit Management Committee will have ultimate responsibility for Information Governance and each year will receive an **Annual Information Governance Report** from the Information Governance Lead, including a review of any changes required to this Information Governance Policy and a summary of the Information Governance Improvement Plan.

4 Scope

4.1 Personnel

This Policy is applicable to all Unit employees, those otherwise employed in the Unit, honorary members, academic visitors, students and contractors.

4.2 Systems

It covers, but is not limited to, any systems or data attached to the Unit's computer or telephone networks, any systems supplied by and operated by or on behalf of the Unit, any communications sent from the Unit, and any data which is owned by the Unit (or the University on behalf of the Unit) held on systems external to the Unit's network. This includes all research data for which the Unit is responsible.

4.3 Information types

This Policy covers all types of information (both paper and electronic), including but not limited to:

- Personnel information
- Organisational/corporate information
- Personal data (see section 2)
- Sensitive personal data (see section 2)

5 Principles and policies

5.1 Principles

The Unit recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Unit places importance on the confidentiality of, and security arrangements to safeguard, personal information about research participants and staff, as well as commercially and academically sensitive information (e.g. emerging study results prior to publication). The Unit also recognises the importance of openness and appropriate sharing of research data.

All information should be appropriately secured throughout its full lifecycle to protect against breaches of confidentiality, failures of integrity, or interruptions to the availability of that information, and to ensure appropriate legal, regulatory and contractual compliance.

5.2 Policies

The Unit will use all appropriate and necessary means to ensure that it maintains and complies with policies in the following areas:

5.2.1 Data Protection

The Unit must comply with the Data Protection Act (1988) and associated Codes of Practice issued by the Information Commissioner's Office and as part of the University of Oxford, the Unit must comply with the University policy on Data Protection. University of Oxford holds the Data Protection Registration number Z575783X.

5.2.2 Freedom of Information

The Unit must comply with the Freedom of Information Act (2000) and associated Codes of Practice issued by the Information Commissioner's Office. As part of the University of Oxford, the Unit must comply with the University policy on Freedom of Information (see Appendix III).

5.2.3 Acceptable Use of Information Technology Facilities

As part of the University of Oxford, the Unit must comply with the University Regulations relating to the use of Information Technology Facilities and with a range of regulations and policies applying to all users of University Information and Communications Technology facilities (see http://www.ict.ox.ac.uk/oxford/rules/).

5.2.4 Information Security

As part of the University of Oxford, the Unit must comply with the University policy on Freedom of Information (see Appendix III). This is enacted through the Unit's Information Security Policy (see Appendix II), which must be reviewed annually and approved by the Unit Management. The Unit IT and Security Manager should be contacted if specialist advice on Information Security is required.

5.2.5 Sharing of Research Data

The Unit should comply with the Medical Research Council Policy and Guidance on Sharing of Research Data from Population and Patient Studies (see Appendix III). A specific Unit Data Access Policy (see Appendix II) has been developed by the Unit that enables appropriate sharing of research data, while emphasising the need to protect participants, honour the Unit's commitments to them and act within the scope of their informed consent and to ensure compliance with legal and regulatory requirements (e.g. the Data Protection Act 1998). The unit's policy on data sharing should be consistent with any such policy implemented by the parent department, the Nuffield Department of Population Health.

5.2.6 Additional policies and procedures

In order to fulfil the intentions of this Unit Information Governance Policy, a number of subsidiary policies and procedures should be maintained (see Appendix II). Unless otherwise stated, these should be approved by the Information Governance Committee with copies provided to the Unit Management Committee (as well as dissemination to all relevant staff).

5.3 Information Asset Register

Information Assets should be documented in a register, which should be developed, maintained and reviewed under the oversight of the Senior Information Risk Owner. All critical Information Assets must be identified and included in this register, together with details of their criticality, the Information Asset Owner, and the risk reviews carried out. Components that relate to the same information asset or business process may be grouped together (e.g. an IT system, its documentation, its physical location, the data held within it and the skills of staff who administer may be grouped as a single Information Asset). Information Asset Owners are responsible for providing these details (including any changes or updates) promptly to the Senior Information Risk Owner.

5.4 Interpretation

Where this policy (or any of the supporting policies; see Appendix II) is thought to be unclear, the Information Governance Lead may issue clarifications. Such clarifications will inform the next review of the policy.

6 Information Governance Management and Responsibilities

6.1 Organisational structure

The organisational structure and management of the Unit is described in Appendix I.

6.2 Key roles

6.2.1 Unit Management Committee

The Unit Management should actively support Information Governance throughout the Unit. Key responsibilities are:

- to review and approve (changes to) the Information Governance Policy
- to provide the resources and funding needed for Information Governance
- to approve assignment of specific roles and responsibilities for Information Governance as described in Appendix I

6.2.2 Information Governance Committee

The Information Governance Committee should comprise senior representatives from across the Unit. The Information Governance Committee should play a central role in the development of best practices which are acceptable, practicable, 'owned' and therefore supported across the Unit. It should also influence the integration and inclusion of Information Governance standards with other governance, strategies, work programmes and projects (e.g. individual research studies or IT programmes).

Terms of Reference for the Information Governance Committee are set out in Appendix IV.

6.2.3 Information Governance Lead

The Information Governance Lead is accountable to the Unit Management and is responsible for ensuring effective management, accountability, compliance and assurance for all aspects of Information Governance, including:

- ensuring a co-ordinated approach to Information Governance across the Unit
- identifying best practice, defining and delivering improvement plans
- working closely with staff across the Unit (including Information Asset Owners and Unit Management) to ensure that Information Governance requirements set out by this Policy are understood, adhered to and appropriately resourced
- developing and maintaining comprehensive and appropriate documentation relating to Information Governance (including this Policy, relevant supporting policies and procedures,)
- chairing the Information Governance Committee, including establishing working groups as necessary to co-ordinate the activities of staff given Information Governance responsibilities and progress initiatives
- ensuring evaluation and improvement activities (including audits and annual assessments) are carried out, documented and reported
- ensuring that the annual assessment and improvement plans are prepared for approval by the Unit Management
- ensuring that the approach to information handling is communicated to all staff and made available to the public
- ensuring that appropriate training is made available to staff and completed as necessary to support their duties
- liaising with other committees, working groups and organisations in order to promote and integrate Information Governance standards
- providing a focal point for the resolution and/or discussion of Information Governance issues

6.2.4 Senior Information Risk Owner / Information Governance Accountable Officer

The Senior Information Risk Owner (SIRO) should be a member of the Unit Management with overall responsibility for the Unit's Information Risk Policy and all matters relating to Information Governance within the Unit. The SIRO will also lead and implement the information governance risk assessment and advise the Unit Management on the effectiveness of information risk management across the Unit. The key responsibilities of the Senior Information Risk Owner are to:

- oversee the development of an Information Risk Policy (see Appendix II), and a strategy for implementing the policy within the existing Information Governance Framework
- take ownership of the risk assessment process for information risk, including review of an annual information risk assessment
- oversee the maintenance of the Information Asset Register and the processes for risk assessment and management
- review and agree action in respect of identified information risks
- ensure that the Unit's approach to information risk is effective in terms of resource commitment and execution and that this is communicated to all staff
- provide a focal point for the resolution and/or discussion of information risk issues
- ensure that Unit Management is adequately briefed on information risk issues

6.2.5 Information Asset Owner

In relation to the Information Assets under their purview, Information Asset Owners are responsible for understanding and addressing risks to the information, and implementation of this Policy (including relevant supporting policies and procedures; see Appendix II). This includes:

- being aware of what information is held, and the nature of and justification for information flows to and from the assets for which they are responsible;
- controlling access to the Information Asset;
- ensuring that all personnel working with that Information Asset are aware of their responsibilities
- ensuring information is used in compliance with this Policy;
- providing assurance to the Senior Information Risk Officer that information risk is being managed effectively; and
- providing or informing annual written reports to the Senior Information Risk Owner on the assurance and usage of their asset

For the purposes of Information Governance, Information Asset Owners are directly accountable to the Senior Information Risk Owner. Information Asset Owners may be assisted in their roles by staff acting as Information Asset Administrators, i.e. staff who have day-to-day responsibility for management of information risks affecting one or more assets.

Unless explicitly stated otherwise, Information Asset Owners are determined as follows:

Information Asset	Information Asset Owner
Research study[1]	Principal Investigator
Administrative information[2]	Unit/ Department Administrator

IT infrastructure[3]	IT and Security Manager
All other information	Unit Director[4]

[1] Examples include MWS, EPIC, DSW

[2] Examples include personnel files, unit accounts

[3] Examples include servers, firewall, networking

[4] or nominated deputy (e.g. Deputy Director)

6.2.6 Line Managers

All Line Managers are responsible for the implementation of this Policy (including relevant supporting policies and procedures; see Appendix II) within their area of responsibility and for ensuring that all staff under their line management are (a) made fully aware of the policy; and (b) given appropriate support and resources to comply.

6.2.7 Individual Personnel

It is the responsibility of each individual within the Unit to adhere to the Information Governance requirements incumbent upon them and to ensure that they comply with these on a day-to-day basis. In particular, if they become aware of actual or potential breaches of the policy, they must bring these to the attention of their Line Manager, the Information Asset Owner or the Information Governance Lead.

7 Training

The Unit is committed to providing education and training, and generating awareness of the importance of Information Governance to ensure that all Unit personnel (including staff and students) are aware of their responsibilities.

7.1 Induction

All staff should receive, as part of their induction, a training session on Information Governance, and attendance should be documented. During the induction process, the new employee must be taken through the Regulations and Policies applying to all users of University ICT facilities (http://www.ict.ox.ac.uk/oxford/rules/) and are then required to sign to indicate agreement, understanding and intended conformance.

7.2 Additional training

The Unit is committed to providing Information Governance training relevant to the role of the individual. In particular, the Unit must ensure that key Information Governance staff (e.g. Information Governance Lead, Senior Information Risk Owner, IT & Information Security Manager, Information Asset Owner) have access to training relevant to their role (e.g. through the Information Governance Training Tool developed by the Health and Social Care Information Centre). Additional, specific training should be provided for those undertaking specialist roles (e.g. those with particular involvement in the maintenance of information security systems). All Unit staff have access to a wide range of training courses offered by the University. In addition, staff may apply to attend external training courses that are appropriate to their role.

The Unit should actively promote awareness of Information Governance within the Unit and provide access to relevant resources.

8 Personnel

8.1 Job descriptions and contracts

All personnel must have a confidentiality and security statement included in their contract of employment. Where appropriate, security and confidentiality responsibilities should be defined in the job description for a role.

8.2 Recruitment procedures

References should be sought before a formal offer of employment is made. New employees should be on probation initially and their work should be monitored by their line manager or an assigned mentor. Any temporary staff must be vetted either by the Unit Personnel Officer or by the external agency holding their contract. All temporary staff must sign confidentiality and acceptable use agreements. Those staff whose role requires access to University finance or personnel systems should be checked with Disclosure Scotland prior to being given such access.

8.3 Disciplinary measures

Failure to comply with this policy (and any related or subsidiary policies, see Appendix II and III) that occurs as a result of deliberate, malicious or negligent behaviour should result in disciplinary action.

9 Sub-contracting

Relevant provisions of this Information Governance Policy must be included in all sub-contracts (including with academic collaborators or institutions, suppliers, or service organisations).

10 Evaluation and improvement

10.1 Monitoring compliance

10.1.1 Review against reference standards

The Information Governance Lead is responsible for ensuring that the Information Governance Policy (and related policies and procedures) are in compliance with relevant reference standards, including existing and new external policies (see Appendix III), laws and regulations. This review should include a self-assessment of compliance with the Information Governance Toolkit.

10.1.2 Audits and inspections

The Unit should undertake audits of compliance with the policies and procedures relating to Information Governance on a regular basis. These may be conducted by staff internal to the Unit (e.g. organised by the Information Governance Committee), by other groups within the University (e.g. by relevant Departmental or central University Information Governance organisations), or external (e.g. commissioned external audits, or inspections by relevant regulators).

10.2 Incident management

The Unit will follow the University's advice for the escalation and reporting of security incidents. Information breaches that involve personal data will subsequently be reported to the University's Data Protection Officer. All Information Governance incidents or other breaches of this policy (including subsidiary policies) will be recorded, and a report of the number of such breaches and their type will be provided on a regular basis to the Unit Management.

10.3 Improvement planning

The Information Governance Committee is responsible for formulating an Information Governance Improvement Plan each year. This should detail the actions that have been raised through the above monitoring activities, along with a timeline and assessment of the risks and benefits of such changes. The Information Governance Improvement Plan must form part of the Information Governance Lead's annual report to Unit Management (see section 11).

11 Reporting

11.1.1 Ad hoc Information Governance Incident Management Reports

The Information Governance Lead is responsible for providing the Unit Management with timely reports of Information Governance events or incidents, together with any recommendations for remedial action and/or Information Governance improvements (see Information Governance Incident Management Policy; Appendix II)

11.1.2 Annual Information Governance Report

The Information Governance Lead is responsible for providing the Unit Management with an Annual Information Governance Report, including:

- A listing of all Information Governance events or incidents (including actual and potential breaches of confidentiality or information security)
- A review and (if necessary) updated version of this Information Governance Policy
- A revised and updated Information Governance Improvement Plan

12 Policy review and revision

This Information Management Policy must be reviewed at least annually and more frequently if required to make improvements in response to routine audits (internal or external) or incident management findings. Any changes to the policy should be reviewed by the Unit Management Committee for approval.

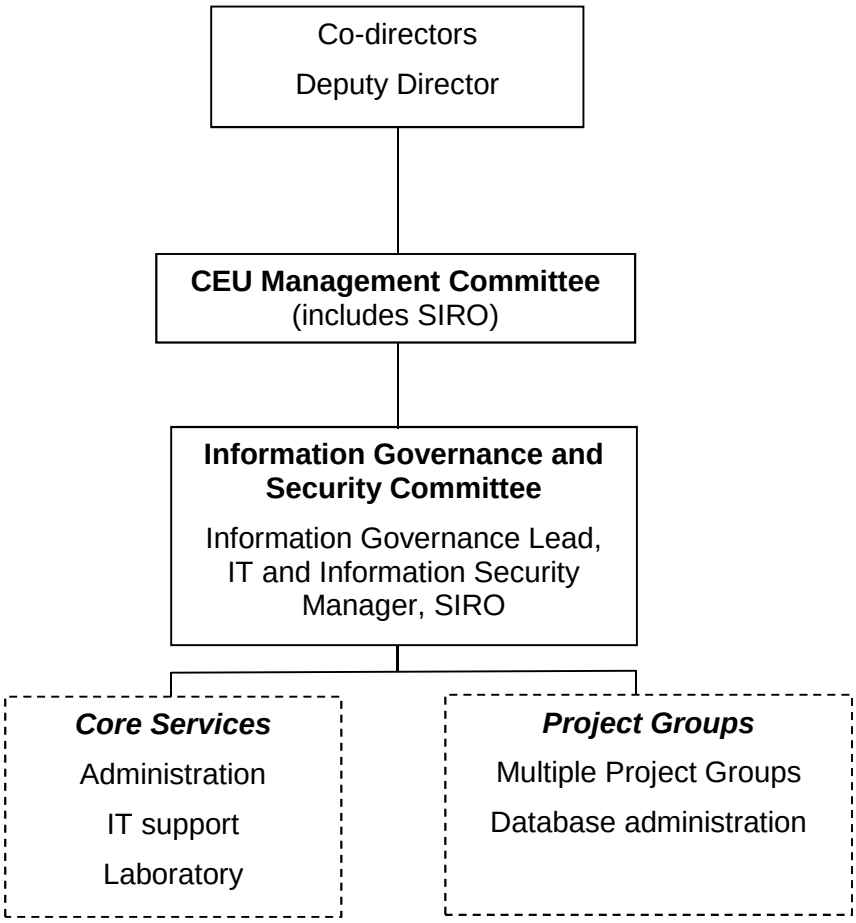
Ownership, review frequency and approver requirements for other and subsidiary Unit policies are summarised in Appendix II.

13 Appendix I – Unit organisation and management

13.1 Place within University departmental and divisional structure

The Cancer Epidemiology Unit (CEU) is a medical research and teaching unit within the Nuffield Department of Population Health. The Nuffield Department of Population Health sits within the Medical Sciences Division of the University of Oxford.

13.2 Unit Organisation Chart



SIRO: Senior Information Risk Owner

13.3 Management structure

CEU has two Co-Directors and a Deputy Director. The Co-directors chair the CEU Management Committee, which oversees the running of the Unit. The Information Governance and Information Security Committee is responsible for the development and implementation of CEU policies on Information Governance and Security. The structure of CEU is divided broadly into Core Services and Project Groups. Each project group is responsible for the organisation, administration, data collection, data validation and integrity for a particular study. The groups that form the Core Services support the Project Groups for day-to-day operation.

13.4 Roles and responsibilities

Role/responsibility	Identity
Unit Management Committee	CEU Senior Management Committee
Unit Co-directors	Prof Dame Valerie Beral & Prof Jane Green
Unit Deputy Director	Prof Tim Key
Unit/Dept Administrator	Ms Isobel Lingard/ Ms Ana Fortun
Information Governance Lead	Dr Lucy Wright
Senior Information Risk Owner / Information Governance Accountable Officer	Prof Jane Green
IT and Security Manager	Mr Dave Ewart

14 Appendix II – Relevant unit policies

14.1 Unit Policies

The following policies require approval by Unit Management, typically on an annual basis (as defined in the individual policies):

Title: Location:	Information Security Policy v:\IG_policies
Title: Location:	Data Access & Sharing Policy http://www.millionwomenstudy.org/data_access/ http://www.epic-oxford.org/data-access-sharing-and-collaboration/

14.2 Subsidiary policies

The following policies are subsidiary to this Information Management Policy and require approval by the Information Governance Committee

Title: Location: Owner: Approver: Review:	Information Security Incident Reporting and Management v:\IG_policies Information Governance Lead Information Governance Committee Annual
Title: Location: Owner: Approver: Review:	Protection and Transmission of Personal Information v:\IG_policies Information Governance Lead Information Governance Committee Annual
Title: Location: Owner: Approver: Review:	De-identification v:\IG_policies Information Governance Lead Information Governance Committee Annual
Title: Location: Owner: Approver: Review:	Confidentiality audit v:\IG_policies Information Governance Lead Information Governance Committee Annual

15 Appendix III – Relevant external policies

The following policies have been developed and are owned by organisations outside the Unit.

15.1 University policies

Policy
University of Oxford policy on Data Protection http://www.admin.ox.ac.uk/councilsec/compliance/dataprotection/
University of Oxford policy on Freedom of Information http://www.admin.ox.ac.uk/councilsec/compliance/foi/
University of Oxford Information Security Policy http://www.it.ox.ac.uk/policies-and-guidelines/information-security-policy
University of Oxford Regulations Relating to the use of Information Technology Facilities http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml
Regulations and Policies applying to all users of University ICT facilities http://www.ict.ox.ac.uk/oxford/rules/

15.2 Other policies

Policy
Medical Research Council Policy and Guidance on Sharing of Research Data from Population and Patient Studies http://www.mrc.ac.uk/news-events/publications/mrc-policy-and-guidance-on-sharing-of-research-data-from-population-and-patient-studies/

16 Appendix IV – Information Governance Committee Terms of Reference

16.1 Accountability

The Information Governance Committee is accountable to the Unit Management.

16.2 Responsibilities

The Information Governance Committee is responsible for assisting the Information Governance Lead in the following activities:

- Ensuring that the Unit has effective policies and management arrangements covering all aspects of Information Governance in line with the Unit's overarching Information Governance Policy.
- Ensuring that the Unit undertakes or commissions assessments and audits of its Information Governance policies, procedures and activities.
- Establishing an Annual Information Governance Improvement Plan, securing the necessary resources and monitoring the implementation of that plan
- Receiving and considering reports into breaches of confidentiality and/or security, and ensuring that appropriate remedial action is taken
- Providing necessary reports to the Unit Management (including an Annual Information Governance Report)
- Raising awareness of Information Governance within the Unit
- Ensuring that staff are trained in Information Governance, complying with and understanding the consequences of not adhering to the relevant policies
- Keeping abreast of developments in relevant external policy, law or regulation

16.3 Membership

16.3.1 Standing members

The Information Governance Committee should consist of the following members:

- Information Governance Lead (Chair)
- Senior Information Risk Owner
- IT and Security Manager

16.3.2 Co-opted members

For specific projects or activities (e.g. development of a specific policy or review of a particular Information Governance issue), additional members with relevant knowledge, skills or expertise may be co-opted. Examples of such individuals include the Unit Personnel Administrator, University Freedom of Information Officer, IT Systems Administrator, Information Asset Owners and Information Asset Assistants (senior staff as well as study coordinators, database managers).

16.4 Frequency of meetings

At least 3 times per year