Imperial College
London

Imperial College

Information Governance Policy Framework

Doc. Ref.	: Information Governance Policy Framework
Version	: 2.0
Status	: Approved
Date	: 20/04/2018
Approved by	: The Provost Board
Review by	: 30/04/2019

1. INTRODUCTION

1.1 This document constitutes the Imperial College London Information Governance Policy Framework (in short, the "Framework"). It gives an overview of the policies, codes of practice and guidelines that apply to information governance at the College; it also sets out the College's commitment to providing information governance training and increasing awareness in this area.

1.2 This Framework pulls together all the requirements for information governance so that all College information is processed legally, securely, efficiently and effectively. Information plays a key part in the College's day to day operations and governance. The quality of the College's services, planning, performance measurement, assurance and financial management relies upon accurate and available information. Robust information governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. Accordingly, this Framework sets out the requirements, standards and best practice that apply to the handling of information.

1.3 Information governance is a key responsibility of each and every member of the College's community. Everyone has a part to play in implementing and embedding our policies and codes of conduct into the College's working practices. So, College staff and students must familiarise themselves with this Framework and the policies it describes. This Framework and the information governance it sets are also expected of any third parties handling College information.

1.4 The aim of this Framework is to help the College:

- comply with its legal, regulatory and contractual obligations;
- maintain robust corporate governance;
- deliver high quality services;
- deliver value for money and protect the public funds entrusted to it;
- put in place appropriate business continuity arrangements;
- continuously improve the way we handle, utilise and protect College information.

1.5 The College holds and processes huge volumes of standard and sensitive data (as defined in Section 2.3 below) that is necessary for service provision, commercial engagement, research and the safeguarding of everyone across the College estate.

2. SCOPE

2.1 This Framework covers all information held by the College or on behalf of the College whether in electronic or physical format including by way of example:

- electronic data stored on and processed by fixed and portable computers and storage devices;
- data transmitted on networks;
- information sent by fax or similar transfer methods;
- all paper records;
- microfiche, visual and photographic materials including slides and

CCTV;
- spoken, including face-to-face, voicemail and recorded conversation.

2.2 The following are expected to comply with the Framework:
- all staff, and students of the College;
- any third parties handling, or having access to, College information including for example consultants, service providers and contractors, visitors, volunteers.

2.3 The Framework is split into two parts – the first part describes the College's overarching information governance strategy and the second part sets out the information governance roles and responsibilities, policies and training.

2.4 The following is the classification template in accordance with which most College data can be classified:

(1) personal data - this is defined in Article 4 of the General Data Protection Regulation as any information relating to an identified or identifiable natural person (referred to as a 'data subject'), where an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The collection, use and retention of personal data must comply with strict conditions and such data requires special measures of protection as more particularly described in the College's Data Protection Policy;

(2) sensitive personal data (also known as special categories of data) is a subset of personal data - this is defined in Article 8 of the General Data Protection Regulation as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Medical research data for example is likely to include some sensitive personal data. The processing of sensitive personal data is subject to additional requirements and requires additional protections also as described in more detail in the College's Data Protection Policy;

(3) non-personal data (organisational data) which can be:

a. sensitive organisational data which includes commercially sensitive planning / administrative or research data, data protected by confidentiality agreements, legally privileged information, etc. This data should be protected by appropriate protection measures; and

b. non-sensitive organisational data which is data pertaining to College not published by default, but which may be disclosed (subject to legal advice) in response to requests made under the Freedom of Information Act.

3. INFORMATION GOVERNANCE STRATEGY

3.1 Purpose of the strategy

3.1.1 The aim of this strategy is to enable the College to meet its information management and security responsibilities so that customers, businesses, partners and suppliers have the confidence that information is handled and stored with due regard to its value and risk. Individuals must understand the importance of using information correctly, of sharing it lawfully and of protecting it from improper use.

3.1.2 The intention of this strategy is also to enable the College to meet its legal and ethical obligations in terms of:

- the use and security of personal identifiable information;
- appropriate disclosure of information when required;
- regulatory frameworks for the management of information;
- professional codes of conduct for consent to the recording, sharing and uses of information;
- operating procedures and codes of practice adopted by the College;
- information exchanged with third parties.

3.1.3 The strategy recognises the high standards expected of the College as well as the ongoing task of maintaining appropriate standards of security in the area of information governance and of embedding a security culture fully throughout the College.

3.2 Strategic objectives

These are the overarching information governance objectives of the College. We want:

- information governance at the College to be an enabler to the College's overall strategy as well as to the underlying departmental strategies and business transformation programmes and for information assurance practices to be embedded within the design and implementation of such strategies and programmes;
- the infrastructure and processes for service delivery to provide the right information to the right people at the right time for the right purpose and promote the provision of high quality services by promoting the ethical, legal, effective and appropriate use of information;
- to provide innovative solutions to information governance issues with a view to transforming business processes;
- to promote information governance ensuring that it is embedded throughout the organisation and to direct organisational wide cultural change so that information is regarded as a key asset;
- to build into staff competencies and job descriptions specific requirements around the governance of information;

- to encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- to work to achieve required standards to comply with legislative, regulatory and contractual obligations and relevant policies;
- to identify and support effective practice in the management of information across all business areas, including preventing duplication of effort and enabling efficient use of resources;
- to identify and manage information assets across College and introduce an information risk management regime that balances risks with opportunities;
- to implement and operate proportionate controls that apply best practice standards to protect information assets and give confidence to all interested parties;
- to provide adequate training to all staff and key partners, increase awareness and embed a culture of care and responsibility in the handling of all information throughout the College.

3.3 Approach

3.3.1 Information governance and assurance are integrated into all aspects of College operations. In delivering information governance services, four key elements of College operations will be considered:

- people
- process
- information
- technology

3.3.2 All information governance, improvement and assurance activities will consider how these factors need to operate in combination to achieve our strategic objectives.

3.3.3 The delivery of our information governance strategic objectives will be through a range of projects and a dedicated Information Governance Improvement Programme. The Improvement Programme will define each information governance project, and these will be implemented and monitored in accordance with the stated governance arrangements and the approach detailed within this Framework.

3.4 Benefits

The following benefits (which are not an exhaustive list) provide an overview of the main benefits that should be derived through the delivery of this strategy:

- consistent and effective management of information across the College;
- increased understanding of and compliance with relevant legislation;
- reduced number of information security incidents;
- reduced staff time and effort;
- improved data quality;
- clear responsibilities in relation to Information Governance and Assurance;

- effective management of information risks;
- greater confidence that information risks are effectively managed;
- better management of research data, with protection of intellectual property.

3.5 Strategy Governance

The College Secretary (who serves as the Senior Information Risk Owner - SIRO) is accountable for implementing this strategy. The Information Governance Steering Group (chaired by the College Secretary) is responsible for monitoring and reporting progress on the improvement programme throughout the year.

The information governance strategy will be implemented through the agreed policies, improvement programmes and through wider agreed change projects.

Annually, the Information Governance Steering Group will agree the improvement programme for the coming year, based on agreed priorities and available resources. The SIRO will annually ratify the improvement programme agreed by IGSG.

4. KEY ROLES AND RESPONSIBILITIES FOR INFORMATION GOVERNANCE

The Appendix to this policy includes a diagram showing the key roles and responsibilities for information governance within College.

4.1 College Secretary

The College Secretary is the College's Accountable Officer and Senior Information Risk Owner, who has overall responsibility for ensuring that information risks are assessed and mitigated and who has overall responsibility for disseminating policy and awareness to all who need to know within College. Information risks are handled in a similar manner to other risks, such as financial, legal and reputational risks.

The College's Accountable Officer and Senior Information Risk Owner has delegated authority to the current Director of Information Governance for the Imperial College Academic Health Science Centre - Professor Paul Elliott - to sign on behalf of the College NHS data sharing framework agreements, data processing agreements, data access compliance applications, and such other contracts and agreements as may be required for the College to access and share data required for research purposes.

4.2 Chief Information Officer (CIO)

The CIO is responsible for establishing and maintaining the enterprise vision, strategy and programme to protect information assets and systems. They also act as the Chief Information Security Officer of the College.

4.3 Heads of Department

Heads of Department are responsible for consideration of IG implications across their department and when working with partners. See the Information Security Policy for specific responsibilities relating to information security.

4.4 Data Protection Officer (DPO)

The DPO is the focal point for all activity within the College relating to data protection. See the College's Data Protection Policy for details.

4.5 Data Protection Co-Ordinators (DPCs)

DPCs act as a local contact in the relevant department or division (as is applicable) for more routine data protection queries and guidance. DPCs also help facilitate the dissemination of data protection communications within their department or division.

4.6 Information Asset Owners

Information asset owners are the assigned owners of College information assets as listed in the College's Information Asset Register. They are responsible for assessing information security and data privacy risks annually using the "Code of Practice 1 - Data Privacy Impact Assessment" or an approved alternative form of assessment determined per data provider for their assets and implementing appropriate measures accordingly.

4.7 Information Governance Steering Group (IGSG)

IGSG oversees this Framework and the policies referred to within it, as well as any agreed information governance improvement programmes. Please see: https://www.imperial.ac.uk/admin-services/secretariat/college-governance/governance-structure/information-governance-steering-group/ for Terms of Reference and composition of the group.

4.8 Information Security Steering Group (ISSG) and Information Governance Operational Group (IGOG)

These groups report to IGSG and act as forums to provide advice and propose changes to policies and codes of practice, particularly on changes to information security and on reports of information security incidents, as well as on remedial actions.

4.9 All College Staff and Students and authorised Third Parties

All College staff, students and academics as well as authorised third parties who use and have access to College information must understand their personal responsibilities for information governance and comply with the law. All staff must comply with College policies, procedures and guidance and attend relevant education and training events in relation to information governance.

5. POLICIES WITHIN THE FRAMEWORK

5.1 The Information Governance Policy Framework encompasses the following policies and codes of practice:

Type of document	Reference	Title
Policy	**DP_0**	**Data Protection Policy**
Code of Practice 1	DP_C01	Handling of Personal Data
Code of Practice 2	DP_C02	Handling of Patient Data
Code of Practice 3	DP_C03	Access to Personal Data by Data Subjects
Code of Practice 4	DP_C04	CCTV
Code of Practice 5	DP_C05	Information Asset Register
Policy	**IS_0**	**Information Security Policy**
Code of Practice	IS_C01	Data Privacy Impact Assessment
Code of Practice	IS_C02	Electronic Messaging
Code of Practice	IS_C03	Inspection of Electronic Communications and Data
Code of Practice	IS_C04	Passwords

5.2 Policies at a glance

5.2.1 Data Protection Policy

This policy sets out the College's obligations regarding the personal data it processes.

5.2.2 Information Security Policy

The policy defines responsibilities for everyone in - and working with – the College. It discusses the College's information asset register and information security risk assessments – a key mechanism for managing all information across the organisation. It discusses the obligation on all staff and students to report information security incidents, and the obligation on the College to provide training to, amongst other things, minimise the risk of such incidents occurring. It discusses the category of sensitive data (which includes personal and commercial data). It also contains the acceptable use requirements of College ICT systems, including discussion on using own devices, and the need for secure disposal of information assets at the end of their lifecycle.

5.3 Policies development

5.3.1 IGSG reviews and recommends changes to all information governance policies. All policies are made available to staff via the internet and are communicated via regular updates to staff.

5.3.2 Existing policies are updated, and new policies introduced in line with requirements, with policies reviewed on an annual basis. These policies must be read in conjunction with staff employment contracts or student regulations as appropriate.

5.3.3 Policies outline scope and intent and provide staff, students and academics with a robust information governance framework whilst setting out their responsibilities. The College is committed to ensuring that all staff and those working with it are familiar with the

organisation's objectives and what is expected in order for these to be achieved. Policies and procedures are one of the key means College uses to communicate these expectations with staff and students.

5.4 Training and development

5.4.1 Information governance training and development is essential for the development and improvement of staff knowledge and skills relating to information governance across the College.

5.4.2 Information governance training must extend beyond basic confidentiality and security awareness in order to develop and follow best practice. Staff must understand the value of information and their responsibility for it, which includes data quality, information security, records management, confidentiality, etc.

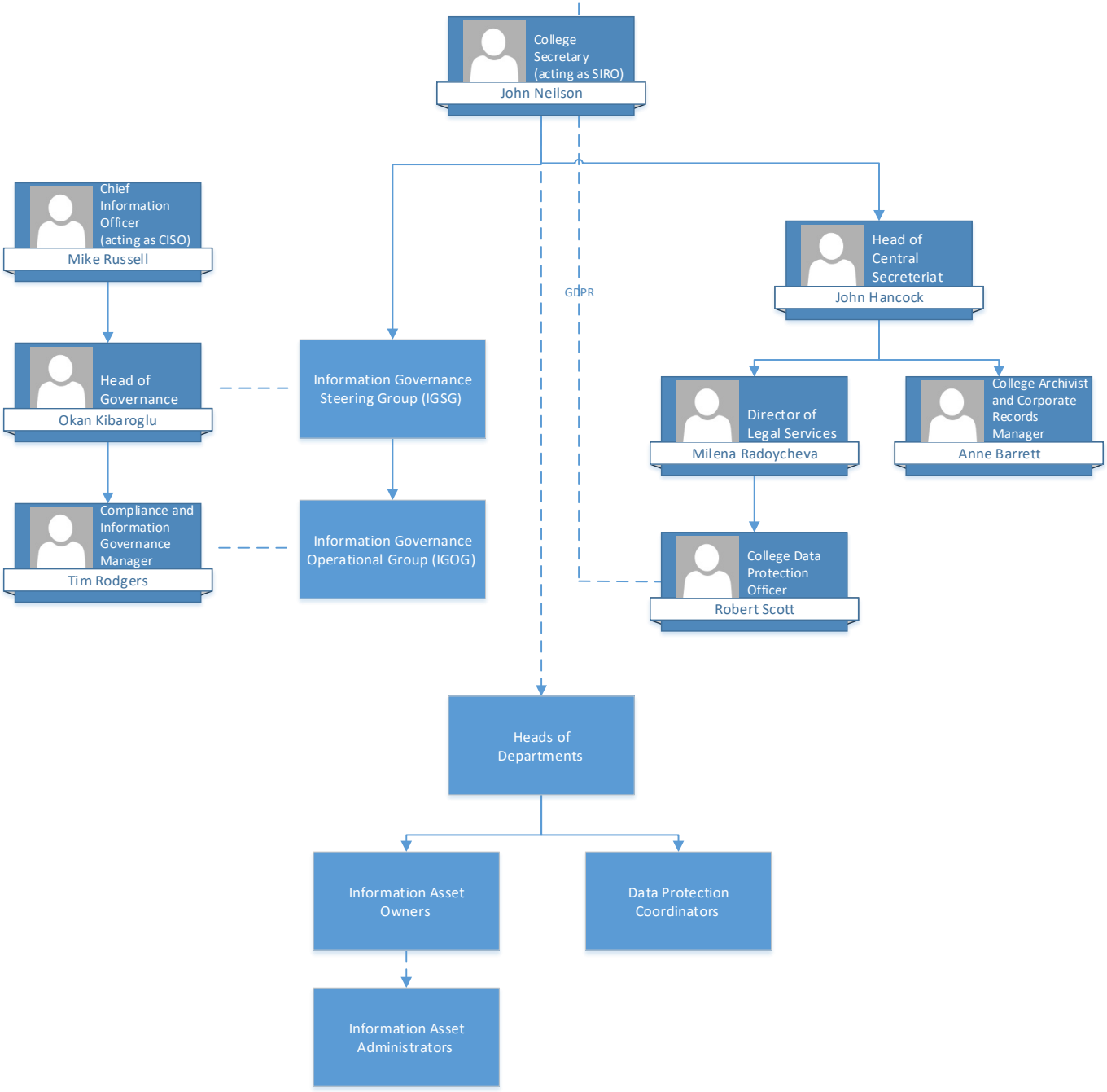
5.4.3 Information governance training is a mandatory requirement for all new staff as part of their induction. Please see the relevant policies for details of mandatory training. More information is also available on the Imperial Essentials pages under Keeping our Information Safe.

6. MONITORING COMPLIANCE WITH THIS FRAMEWORK

IGSG retain overall responsibility for monitoring compliance with this Framework and review of each policy.

Imperial College
London

Appendix: Key Roles and Responsibilities for Information Governance within Imperial College London



Version History

Version/Status	Release Date	Comments
0.1/Draft	June 2016	Initial Draft, reviewed by IGSG members
0.2/Draft	July 2016	
1.0	October 2016	Approved by the Provost Board
1.1/Draft	January 2018	Reviewed by IGOG
1.2/In Review	March 2018	Reviewed by Jon Hancock, Head of Central Secretariat; Milena Radoycheva, Director of Legal Services; Robert Scott, College DPO
1.3	27 April 2018	Approved by the Provost Board