Imperial College
London

Imperial College

Information Governance Policy Framework

Doc. Ref.	: Information Governance Policy Framework
Version	: 4.0
Status	: Approved
Date	: 21/10/2022
Approved by	: The Provost's Board
Review by	: 21/10/2023

1. INTRODUCTION

1.1 The Imperial College London Information Governance Policy Framework (in short, the "Framework") incorporates the College Information Security Policy and the College Data Protection Policy, their related codes of practice and guidance.

1.2 The 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 all College staff and students and authorised third parties carrying out work for or in the College. 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, students and authorised third parties having access to College data must familiarise themselves with this Framework and the policies it covers. To verify understanding of their responsibilities, all College staff and students should complete the Information Security Awareness training and the Data Protection Awareness training every two years.

1.4 The objective 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 significant volumes of standard and sensitive data (as defined in Section 2.3 below) to fulfil its mission providing education and research, and relevant commercial and stakeholder engagement.

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, but not limited to:

- 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;
- Authorised third parties handling, or having access to, College information including for example consultants, service providers and contractors, visitors, volunteers.

2.3 The following is the classification template which should be used for all College data; please see College's Data Protection Policy to find out more about how to protect data in respective categories:

1. Confidential Data:
    a. Sensitive Personal Data: defined as the Special Categories of Data in Article 9 of the General Data Protection Regulation – 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. (This includes patient identifiable data for research purposes.) Additional protection measures are required.
    b. Highly Sensitive Organisational Data: Data, which could cause the College damage or financial loss if exposed, data protected by confidentiality agreements, legally privileged information, etc.
2. Restricted Data:
    a. Personal Data: As defined in Article 4 of the General Data Protection Regulation as any information related to a natural person which can be used to identify them – special measures of protection is required.
    b. Sensitive organisational data includes commercially sensitive planning / administrative or research data, etc. – protection measures are required.

3. Unrestricted Data:
    a. Non-personal data (Organisational data)
    b. Non-sensitive organisational data is data pertaining to College which may or may not be published by default but may be disclosed via freedom of information requests subject to legal advice.

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

Our strategic objectives through implementation of effective information governance are:

- 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 achieved through a range of change initiatives and a dedicated Information Governance Improvement Programme, which is owned and reviewed by the Information Governance Steering Group. 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

- 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 is the Senior Information Risk Owner (SIRO) of the College, and 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 Information Governance Improvement Programme.

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

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

Appendix A includes a diagram showing the key roles and responsibilities for information governance.

4.1.1 College Secretary

The College Secretary is College's Accountable Officer, who has overall responsibility for ensuring that information risks are assessed and mitigated. They assume the role of the Senior Information Risk Owner (SIRO), who has the overall accountability for disseminating policy and awareness to all who need to know. Information risks are handled via College's risk management policy and procedures.

4.1.2 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 act as the Chief Information Security Officer (CISO) of the College.

4.1.3 Heads of Department

Heads of Department are responsible for taking Information Governance into account across all activities of their department, including working with partners. See the Information Security Policy for specific responsibilities relating to information security.

4.1.4 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.

4.1.5 Information Asset Owners (IAO)

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 alternative approved form of assessment determined per data provider for their assets and implementing appropriate measures accordingly.

4.1.6 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 se https://www.imperial.ac.uk/admin-services/secretariat/college-

governance/governance-structure/information-governance-steering-group/ for the Terms of Reference and composition of the group.

4.1.7 Information Governance Operational Group (IGOG)

This group reports to IGSG and acts as a forum to provide advice and propose changes to policies and codes of practice as required, as well as on remedial and improvement actions.

4.1.8 All College Staff and Students and authorised Third Parties

All College staff, students and authorised third parties 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. As stated in paragraph 1.3, they should complete the Information Security Awareness training and the Data Protection Awareness training every two years.

4.1.9 AHSC Director of Information Governance

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

Professor Elliott will also fulfil the role of Caldicott Guardian being responsible for safeguarding the confidentiality of patient information

4.2 Policy Development

4.2.1 The Information Governance Steering Group 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.

4.2.2 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 and student regulations as appropriate.

4.2.3 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 for these to be achieved.

4.3 Policies within the Framework

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	DP_C01	Handling of personal data
Code of Practice	DP_C02	Handling of patient data
Code of Practice	DP_C03	Access to personal data by subjects
Code of Practice	DP_C04	CCTV
Code of Practice	DP_C05	Information Asset Register
Code of Practice	DP_C06	Data Sharing and Integration
Policy	IS_0	Information Security Policy
Code of Practice	IS_C01	Hardware and Software Asset Management
Code of Practice	IS_C02	Electronic Messaging
Code of Practice	IS_C03	Inspection of Electronic Communications and Data
Code of Practice	IS_C04	Account Security Management

4.4 Policies at a glance

4.4.1 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.

4.4.2 Data Protection Policy

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

4.5 Training and Development

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

4.5.2 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.

4.5.3 Information governance training is a mandatory requirement for all new staff as part of their induction. Please see the relevant policies for

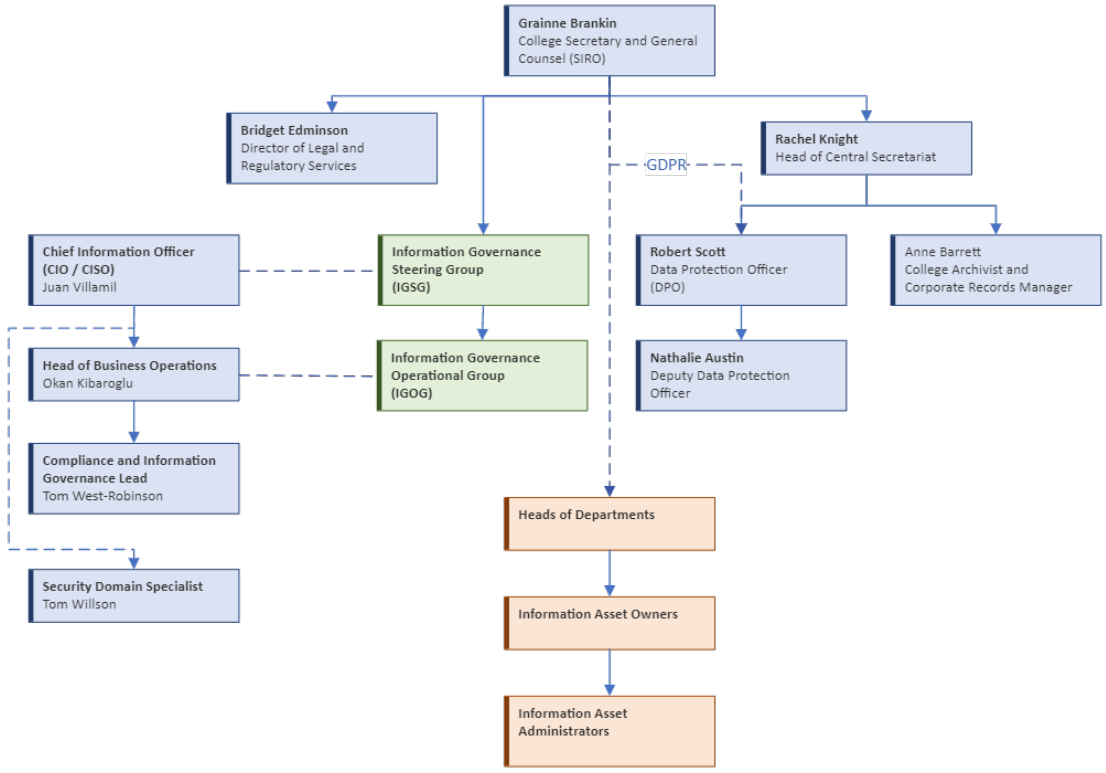
details of mandatory training. More information is also available on the Imperial Essentials web pages.

5. MONITORING COMPLIANCE WITH THIS FRAMEWORK

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

Imperial College
London

Appendix A: Key Roles and Responsibilities for Information Governance



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
2.0/Approved	May 2018	Published version
2.1/In Review	March 2019	Minor changes by Tim Rodgers and Okan Kibaroglu
3.0/Published	April 2019	Approved by IGSG
3.1/In Review	September 2020	Data classification has been revised to a three-level structure. Appendix A has been updated.
3.2/In Review	January 2021	Reviewed by John Neilson, the College Secretary.
3.3/In Review	October 2022	Reviewed by Robert Scott, Okan Kibaroglu, Tom Willson, Tom West-Robinson. Links updated; minor changes to simplify and clarify content. Org chart in Appendix A updated.
4.0/Approved	October 2022	Minor changes confirmed as approved via Rachel Knight, by Robert Scott.