

Information Governance Policy Framework

Introduction

- 1.1 The Information Governance Policy Framework (the “Framework”) incorporates the Information Security Policy / [Information Security Policy](#) [PDF], the Data Protection Policy / [Data Protection Policy](#) [PDF] plus all related codes of practice and associated guidance / [Data Protection and Information Security Codes of Practice](#) [URL].
- 1.2 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 staff, students and authorised third parties carrying out work for or with the university. Everyone has a part to play in implementing and embedding our policies and codes of conduct into the working practices. So, staff, students and authorised third parties having access to data must familiarise themselves with this Framework and the policies it covers.
- 1.4 The objective of this Framework is to help the university:
 - comply with its legal, regulatory and contractual obligations;
 - maintain robust corporate governance measures;
 - 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 access, handle and utilise the information it is responsible for;
 - Support the implementation and completion of risk based and legal documentation, including the completion of Data Protection Impact Assessments (DPIA’s) and Records of Processing Activity (RoPA) entries.
 - Ensure controls are in place to protect, retain and recover information in line with the requirements of the university and wider legislative framework.

1.5 The university holds and processes significant volumes of data (as defined in Section 2.3 below) to fulfil its mission to provide education and undertake research with the framework supporting those aims.

Scope

2.1 This Framework covers all information held by the university or on behalf of the university whether in electronic or physical format including, but not limited to:

2.2 Electronic data stored on and processed by fixed and portable computers and storage devices. This would include storage devices which are owned directly by the university, devices owned by personnel directly and any virtual environments where Imperial data is being utilised or stored;

- 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, video and voicemail where it is recorded;
- Data stored in cloud based models including SaaS, PaaS and IaaS.

2.3 The following are expected to comply with the Framework:

- All staff and students;
- Authorised third parties,

The above individuals have access to Imperial information including that held on behalf of partner organisations (such as commercial and public partners) and includes consultants, service providers, contractors, visitors and volunteers.

Key Roles and Responsibilities for Information Governance

3.1 Deputy University Secretary and General Counsel

The Deputy University Secretary and General Counsel holds 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 risk management policy and procedures.

3.2 Chief Information Officer (CIO)

The CIO leads the Information and Communication Technologies (ICT) division and is responsible for all aspects of Imperial's Digital Plan.

3.3 Chief Information Security Officer (CISO)

The CISO is responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

3.4 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.

3.5 Data Protection Officer (DPO)

The DPO monitors, informs and advises the university regarding its data protection obligations. See the Data Protection Policy for details.

3.6 Information Asset Owners (IAOs)

An Information Asset Owner is a senior role accountable for a defined information asset or data area, with an emphasis on legal compliance and data protection. The IAO's primary responsibility is to ensure that data in their area is handled in line with legislative and institutional policies. This means they oversee how personal data is collected, used, shared, and safeguarded.

3.7 All university staff and students

All university staff, students and authorised third parties must understand their personal responsibilities for information governance and comply with the law. All staff must comply with all policies, procedures and guidance and attend relevant education and training events in relation to information governance.

Policy Development and Overview

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

4.2 Policies outline scope and intent and provide staff, students and academics with a robust information governance framework whilst setting out their responsibilities. Imperial 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.

Policies / Codes of Practice within the Framework

6.1 The Information Governance Policy Framework encompasses all policies and codes of

Practice, including as follows:

Type of document	Reference	Title
Policy	DPA Policy	Data Protection Policy [PDF]
Policy	InfoSec Policy	Information Security Policy [PDF]
Code of Practice		Data Protection and Information Security Codes of Practice [URL]

6.2 Policies at a glance

6.2.1 Information Security Policy

The policy defines responsibilities for everyone in - and working with – the university. It highlights the importance of the information asset register and risk assessments – which are 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 university to provide training to, amongst other things, minimise the risk of such incidents occurring. It discusses the different categories of data (which includes personal and commercial data).

6.2.2 Data Protection Policy

This policy sets out the university’s obligations along with those of its staff and students regarding the personal data it processes. It identified all related Codes of Practice, key staff members and explains key legislative requirements that are placed on the university to uphold and how these are completed.

6.2.3 Data Protection and Information Security Codes of Practice

The Data Protection and Information Security Codes of Practice are formal specific guidelines that outline expected professional conduct by Imperial’s staff and students.

Training and Development

7.1 Data Protection and Information Security training is essential for the development and improvement of staff knowledge and skills relating to information governance across the university.

7.2 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.

7.3 Data Protection and Information Security training is a mandatory requirement for all new staff as part of their induction and must be repeated every two years. More information is available on the [Imperial Essentials](#) [URL] web pages

Document Control

Document title:		Information Governance Policy Framework	
Version:	4.1	Date:	March 2026
Initially approved by and date:		Provost Board July 2016	
Version approved by and date:		Data Protection Officer	
Version effective from:		March 2026	
Originator:		Division of the University Secretary	
Contact for queries:		Data Protection Officer	
Cross References:		Data Protection Policy <ul style="list-style-type: none"> - Data Protection Codes of Practice Information Security Policy <ul style="list-style-type: none"> - Information Security Codes of Practice 	
Notes and latest changes:		V0.1 June 2016 <ul style="list-style-type: none"> - Initial draft created. Reviewed by IGSG V1.0 – October 2016 <ul style="list-style-type: none"> - Version approved by Provost Board V1.2 March 2018 <ul style="list-style-type: none"> - Reviewed and updated published version 2.0 May 2018 V2.1 March 2019 <ul style="list-style-type: none"> - Reviewed by IGOG and updated published version 3.0 April 2019 V3.1 September 2020 <ul style="list-style-type: none"> - Data classification revised - Appendix A updated V3.2 January 2021 <ul style="list-style-type: none"> - Reviewed by College Secretary V3.3 October 2022 <ul style="list-style-type: none"> - Reviewed by IGOG V4.0 October 2022 <ul style="list-style-type: none"> - Minor changes, updated Appendix A and approved by Head of Central Secretariat. V4.1 September 2025 <ul style="list-style-type: none"> - Updated to meet new brand standard. - Job titles and responsibilities amendments where necessary. - Updated personnel and replace IGSG / IGOG references to reflect new committee setup. - Remove references to ‘College’. - Amended list of CoPs and Policies. - Integrated URL’s for various documents. - Amended and updated the Data Classifications list. - Added examples to the Data Classification List. - Amended Appendix A. - Removed names of individuals and replaced with job titles. - Expanded wording within 2.2 regarding data storage / devices etc. to capture non-Imperial and non-physical physical assets. - Removed reference to Caldicott Guardian. - Expanded 6.3 to explain the purpose for the Data Protection and Information Security policies V5.0 March 2026 <ul style="list-style-type: none"> - Owing to changes in the wider Imperial Information Governance framework, the following sections were removed temporarily <ul style="list-style-type: none"> o Section 3 Imperial Business Data Strategy description o Section 4.8 Data Governance Delivery Group description o Appendix A 	