# Information Security Policy

## Introduction

1.1 Information plays a fundamental role in supporting all activities of the university. Properly securing all information that the university processes is essential to the success of its academic and administrative activities. This is to be achieved through managing the three essential attributes of information security: confidentiality, integrity and availability, which are the vital building blocks for safeguarding information.

1.2 The objectives of the Information Security Policy ("the Policy") are to:

1.2.1 enable adequate protection of all of the university information assets against loss, misuse or abuse;

1.2.2 make all users aware of this Policy and all associated policies, Codes of Practice and guidelines;

1.2.3 create an awareness that appropriate security measures must be implemented across the university as part of the effective operation and support of information security;

1.2.4 make all users understand their responsibilities for protecting the confidentiality, integrity and availability of the data they handle.

1.3 This Policy should be read in conjunction with the Data Protection Policy and associated Codes of Practice, which provide more detailed guidance on protecting personal data. The Codes of Practice linked to the policy are:

| Reference | Title / URL |
|---|---|
| Policy | Data Protection Policy / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Data-Protection-Policy.docx |
| ICT CoP 01 | Hardware and Software Asset Management / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/ICT-CoP-01-%E2%80%93-Hardware-and-Software-Asset-Management.pdf |
| ICT CoP 02 | Electronic Messaging / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college- |

| | |
|---|---|
| | governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/ICT-CoP-02---Electronic-Messaging.pdf |
| ICT CoP 03 | Inspection of Electronic Communications and Data / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/ICT-CoP-03---Inspection-of-Electronic-Communications-and-Data-.pdf |
| ICT CoP 04 | Account Security Management / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/ICT-CoP-04---Account-Security-Management.pdf |
| ICT CoP 05 | System Security / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/ICT-CoP-05---System-Security.pdf |
| ICT CoP 06 | Conditions of Use of IT Resources / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/ICT-CoP-06-Conditions-of-Use-of-IT-Resources.pdf |

## Scope

2.1 All staff, students and other authorised third parties including guests, who may have access to information held by or on behalf of the university, must adhere to the Policy and its associated Codes of Practice. The scope of the Policy covers their use of university-owned/leased/rented and on-loan facilities, and all non-Imperial systems, owned/leased/rented/on-loan, when connected to Imperial's network directly or indirectly, to all university-owned/licensed data, services and software, be they on university or on non-Imperial systems, and to all data, services and software provided by sponsors or external agencies.

2.2 As stated in paragraph 2.1 of the Information Governance Framework, the Policy applies to all data held by or on behalf of the university whether in electronic or physical format including:

- 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.

2.3 As explained fully in Section 2.3 of the Information Governance Framework, the following is the Data Sensitivity Classification which should be used for all university data;

2.3.1 Certified Environment Required:

Release of this data would have significant legal and reputational impact on the university. It may be significantly impactful on a large number of individuals.

2.3.2 Confidential Data:

Release of this data would have a high impact on either the university or the individual or it has significant legal restrictions.

2.3.3 Restricted Data:

Release of this data would have a medium impact on either the university or an individual. It is not expected to have significant legal restrictions.

2.3.4 Unrestricted Data:

Release of this data would have a low impact on the university and it could not be tracked back to an individual. It will not have significant legal restrictions.

2.3.5 Public:

There are no impacts from release of this data to the public domain.

2.3.6 Non-sensitive organisational data:

This is data pertaining to Imperial which may or may not be published by default, but may be disclosed via freedom of information requests, subject to legal advice.

2.4 The Policy applies throughout the lifecycle of all information from creation, storage, and use to disposal.

2.5 Although the use of social media resources by university members is unrestricted and not centrally moderated, the university requires its members to ensure they respect this Policy and cause no damage to Imperial's reputation. For further information, refer to web guides on Social Media and Collaboration Policy via https://www.imperial.ac.uk/staff/tools-and-reference/web-guide/policies-and-guidance/comments/.

## Responsibilities

3.1 The key roles and responsibilities at Imperial with respect to information governance are set out in the Information Governance Policy Framework (see section [4]). Of particular importance for compliance with this Policy are:

3.1.1 Heads of Department

Heads of Department have responsibility to ensure that staff, students and other authorised individuals within their department or division are informed of, and comply with this Policy, particularly section 11: Conditions of Use of IT Resources, and the associated Codes of Practice. They are also responsible for ensuring that all information assets held by their departments or divisions are included in the Information Asset Register and an Information Asset Owner is assigned for every information asset.

3.1.2 Staff, students and authorised third parties

All staff, students and authorised third parties must adhere to this Policy and associated Codes of Practice. Compliance with the Policy forms part of the Core Terms and Conditions of Service for staff and forms part of the Regulations for Students. Section 11 of this policy, "Conditions of Use of IT Resources (Acceptable Use Policy)" is displayed and must be accepted by all staff and students before they can start using their username. Any actual, or suspected, information security incidents (such as accidental exposure or loss, unauthorised access, computer virus, malicious software) must be reported to the ICT's Service Desk immediately. Concerned individuals may contact any senior members of ICT or the university directly. (See section 7.1 for their contact details.)

3.1.3 Chief Information Officer

The Chief Information Officer leads the Information Communication Technologies (ICT) Division and is responsible for all aspects of Imperial's Digital Plan. The Chief Information Officer or Chief Information Security Officer (CISO) may decide to audit systems to identify and mitigate risks, or to make inaccessible/remove any unsafe user/login names, data and/or programs on the system from the network.

## Compliance with legislation

4.1 Imperial has an obligation to abide by all UK legislation and relevant legislation of the European Community. Of particular importance in this respect are;

- the Computer Misuse Act 1990;
- The Regulation of Investigatory Powers Act 2000;
- the UK General Data Protection Regulation;
- Data Protection Act 2018; and

- "Prevent Duty Guidance" as directed by the Counter-Terrorism and Security Act 2015.

4.2 The requirement for compliance devolves to all users, who may be held personally responsible for any breach of the legislation. Failure of an individual student or member of staff to comply with this Policy, or with any legislation, may lead to the instigation of the relevant disciplinary procedures as set out in the employment terms and condition and staff policies and the university regulations for students. Failure of a contractor to comply could lead to the termination of a contract. In certain circumstances, legal action may be taken.

**Data Asset Registration Tool (DART)**

5.1 DART is the university's online platform for capturing and creating its Information Asset Register and Data Privacy Impact Assessments respectively. Use of DART is described in the associated code of practice as follows:

5.1.1 Information Asset Register / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/DPA-CoP-05---Information-Asset-Register.pdf

5.1.2 Data Protection Impact Assessment / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/DPA-CoP-07---Data-Protection-Impact-Assessment.pdf

**Monitoring electronic communications**

6.1 In accordance with the "Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000", made under the "Regulation of Investigatory Powers Act 2000" (RIPA) 2000, the university will exercise its right to intercept and monitor electronic communications received by and sent from the university for the purposes permitted under those Regulations. The purposes cover, but are not limited to, monitoring for criminal or unauthorised use, viruses, threats to the system, e.g. hacking and denial of service attacks, ensuring the effectiveness of its operations and compliance with policies and regulations. The monitoring process will be carried out in accordance with "Code of Practice 3: Inspection of Electronic Communications and Data".

**Information Security Incidents**

7.1 Notification of Security / Data Incidents;

a. Anyone who suspects that there has been, or is likely to be, an information security incident, such as a breach of confidentiality, availability, integrity of information, or misuse of an information asset, must be reported to ICT / Cyber Security Office via the ICT Service Desk - https://www.imperial.ac.uk/admin-services/ict/contact-ict-service-desk/. If a person is unable to notify via the Service Desk directly, they may also contact any senior members of ICT or the university directly. Refer to these locations for contact details: https://www.imperial.ac.uk/admin-services/ict/about-ict/meet-the-team/, the Provost or, if not available, the Chief Information Officer, has the authority to take whatever action is deemed necessary to protect the university against breaches of security.

Furthermore, if the incident involves accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, this must be reported immediately to the Data Protection Team via https://www.imperial.ac.uk/admin-services/governance/policies-and-guidance/data-breaches/.

b. If the incident involves cardholder data (CHD) or cardholder data environment (CDE) as described in the Payment Card Industry Data Security Standards (PCI DSS) requirements, use the PCI DSS Incident Response procedure to report it: https://www.imperial.ac.uk/finance/financial-services/controls--compliance/pci-dss/incident-reporting/.

7.2 If a data incident has not taken place, but you believe Imperial may be vulnerable to an incident happening, you should report your concerns about actual or potential information/data vulnerabilities to the Cyber Security Office via the report a vulnerability page https://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/contact-ict-security/

7.3 In the event of a suspected or actual information security incident or an unacceptable network event, the Chief Information Officer or the Chief Information Security Officer may decide to take any action necessary to remedy the situation. This may include blocking access by users to systems, investigating data/events stored in ICT services and examination of any devices connected to the network.

7.4 Failure to report an information security incident or data breach immediately may lead to disciplinary action being taken. If you are in any doubt about whether to report an incident, you should seek advice from ICT or the Data Protection Officer.

**Security Education and Training**

8.1 New users of IT facilities, staff, students and approved third parties, should be instructed on the policies and Codes of Practice relating to information security. They should also be given training on the procedures relating to the security requirements of the particular work they are to undertake and on the correct use of IT assets in general before access to IT services is granted. It is the responsibility of managers to ensure that their staff are suitably trained, and to maintain training records. They should be made aware of this Policy including the reporting procedures in section 7.

8.2 All new staff must complete the Information Security Awareness training and the Data Protection Awareness training, which are included within Imperial Essentials. Staff are also strongly advised to attend the cyber security inductions when joining the university and must be aware of the latest https://www.imperial.ac.uk/admin-services/ict/self-service/be-secure/.

8.3 Staff are required to refresh the Information Security Awareness and Data Protection Awareness training every two years.

**Security considerations for employment**

9.1 Security roles and responsibilities, as laid down in this Policy and related Codes of Practice, should be included in job descriptions, where appropriate. These should include any general

responsibilities for implementing the Policy as well as any specific responsibilities for the protection of assets, or for the execution of particular security processes or activities.

9.2 Applications for employment or changes of role may require screening based on the Pre-employment Checks section of HR's Recruitment and Selection Procedure.

9.3 Agency staff and approved third party users of information systems will be required to sign a confidentiality or non-disclosure agreement as part of their contract as well as a data sharing agreement where they will have access to personal data.

**Protecting High Risk Data**

10.1 It is essential that Imperial protects high risk data. This includes Special Category Data and data that is described as Certified Environment Required Data and Confidential Data (see 2.3) with enhanced security measures.

10.2 High Risk Data must not be stored on or communicated through services which are not provided by the University such as personal email (Gmail, Hotmail etc…) or personal web-based 'cloud' storage services (e.g. Google Apps, Dropbox).

10.3 For guidance on protecting special High Risk Data , refer to the Data Protection Policy / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Data-Protection-Policy.docx and the Be Secure / https://www.imperial.ac.uk/be-secure/ pages on the Imperial website.

10.4 Where possible, data should be anonymised or pseudonymised to remove personal identifiers, especially where patient/participant identifiable data is considered. Any anonymisation used should be risk assessed for effectiveness and documented with Imperial having an anonymisation form in place to undertake the process / https://imperiallondon.sharepoint.com/:w:/r/sites/cf/DPIA/Shared Documents/Templates/Template - Anonymisation Form.docx?d=w0cef1415cbd84a60bea6eb91d7021841&csf=1&web=1&e=2v64tD

10.5 Data must be protected using additional security practices including Multi-Factor Authentication (MFA), access controls and using the principle of least privilege. For further information please see ICT CoP 04 / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/college-governance/charters-statutes-ordinances-regulations/policies-regulations-codes-of-practice/information-systems-security/ICT-CoP-04---Account-Security-Management.pdf

10.6 Data files must be encrypted both at rest and in transit. For more information, refer to ICT's Encrypt Sensitive Information pages via https://www.imperial.ac.uk/be-secure/ and https://www.imperial.ac.uk/admin-services/governance/policies-and-guidance/data-protection-and-information-security-codes-of-practice/.

10.7 Databases and computers containing High Risk Data must be encrypted and require users to input credentials to access the data.

10.8 All devices must be securely wiped before being disposed of. More information is available from ICT on how to dispose of hardware.

**Document Control**

| | |
|---|---|
| **Document title:** | Information Security Policy |

| | | | |
|---|---|---|---|
| **Version:** | 8.0 | **Date:** | 18/12/2025 |
| **Initially approved by and date:** | Senate October 2013 | | |
| **Version approved by and date:** | University Management Board / 8 December 2025 | | |
| **Version effective from:** | December 2025 | | |
| **Originator:** | Registrar & University Secretary | | |
| **Contact for queries:** | Chief Information Security Officer | | |
| **Cross References:** | Information Governance Policy Framework<br>CoP 01 – Hardware and Software Asset management<br>CoP 02 – Electronic Messaging<br>CoP 03 – Inspection of Electronic Communications and Data<br>CoP 04 – Account Security Management<br>CoP 05 – System Security<br>CoP 06 - Conditions of Use of IT resources | | |
| **Notes and latest changes:** | January 2013 / V1<br>- Approved<br>March 2016 / V2.0<br>- UK Legislation in paragraph 14 have been updated; "Prevent" act added.<br>April 2016 / 2.1<br>- Comprehensive revision as per findings report of the Information Governance Audit in 2015. Reviewed by Prof Alan Boobis, Jess Silver (College Data Protection Officer), Dr John Shemilt (Director of ICT), Matthew Williams (Network and Security Manager), ICT Security Team.<br>May 2016 / 2.2<br>- Reviewed by ISSG, Mike Russell and revised accordingly<br>June 2016 / 2.3<br>- Reviewed by John Neilson, College Secretary and Mike Russell, CIO<br>July 2016 / 2.4<br>- Reviewed by IGSG<br>November 2016 / 3.0<br>- Published following Provost Board Approval<br>January 2018 / 3.1<br>- Review by IGOG members<br>March 2018 / 3.2, 3.3 & 4.0<br>- Review by Jon Hancock, Head of Central Secretariat, Milena Radoycheva, Head of Legal Services, and Robert Scott, College DPO.<br>- Submitted to the Provost Board<br>- Published following Provost Board approval<br>March 2019 / 4.1<br>- Annual review carried out by Tim Rodgers and Okan Kibaroglu and Matthew Williams<br>April 2019 / 5.0<br>- Reviewed by IGSG<br>May 2020 / 5.1<br>- All references to IT Director replaced with Chief Information Officer. Additional clarification regarding software piracy added<br>July 2020 / 5.2<br>- Moved CoP 1 related to DPIA to Data Protection Policy; new CoP 1 added "Hardware and Software Asset Management". Contents of Paragraph 5 IAR and DPIA are moved to the Data Protection Policy.<br>January 2021 / 5.3 & 6.0<br>- Reviewed by John Neilson, the College Secretary.<br>- Confirmed to be published by John Neilson<br>June 2021 / 6.1<br>- Multi Factor Authentication added<br>April 2022 / 6.2<br>- 2.3.1 - replaced current classification wording to new wording found in updated Information Governance Framework 4.1 amended reference / hyperlink of EU GDPR to the UK GDPR 5. Updated to reference DART 7.1 PCI DSS incident reporting statement added 8.2 changed word | | |

| | |
|---|---|
| | 'should complete' to 'must complete' as per Imperial Essential requirements 10 Amended to change 'sensitive' to 'special category' which is the legal terminology 11.8.13 PCI DSS policies referred to as a requirement for those involved in PCI DSS processes<br>June 2022 / 7.0<br>- Reviewed and approved by the Information Governance Steering Group.<br>August 2025 / V8.0<br>- Reviewed by ICT / ICT Security and DPO<br>- Updated to meet new brand standard<br>- Referenced the updated and newly renamed 'Data Sensitivity Classification' categories<br>- Integrated URL's into 1.3.<br>- Corrected / added URLs where required to be updated<br>- Updated Section 2 to align with Information Governance Policy Framework data types<br>- Referenced DART in 5.1 as introduction to DPIA and IAR CoPs.<br>- Reworded Section 7.2, content / context remains the same<br>- Erased section 11 'Conditions of use of IT resources (Acceptable use policy)' as this has since been intended to be turned into a standalone CoP.<br>- Integrated anonymisation form link into section 10<br>- Updated the Incident Response process to align between Information Security incidents and Data Protection Incidents<br>November 2025 / V8.0<br>- Proposed changes reviewed by Audit and Risk Committee<br>December 2025 / V8.0<br>- Approved by University Management Board |