Data Protection Policy

Introduction

1.1 Imperial College London needs to collect, store and process personal data in order to carry out its functions and activities. The university is a Data Controller for most of the personal data it processes and is committed to full compliance with the applicable data protection legislation including Data Protection Act 2018, the UK General Data Protection Regulation (GDPR) as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003.

1.2 This Data Protection Policy ("the Policy") should be read in conjunction with the Information Security Policy and related Codes of Practice. These provide more detailed guidance on the correct handling of personal data and together with this Policy are an integral part of the overall information governance framework.

The relevant data protection codes of practice linked to the policy are:

Reference	Title / Link
DP_C01	Handling of Personal Data / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/DPA-CoP-01---Handling-of-Personal-Data.pdf
DP_C02	Body Worn Camera / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/DPA-CoP-02---Body-Worn-Camera.pdf
DP_C03	Access to Personal Data / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/DPA-CoP-03---Access-to-Personal-Data.pdf
DP_C04	CCTV / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/DPA-CoP-04---CCTV.pdf
DP_C05	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
DP_C06	Internal Sharing and Integration / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/DPA-CoP-06---Internal-sharing-and-Integration.pdf

DP_C07	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

1.3 The university's Data Protection Team (within the Information Management & Compliance Team) is led by the university's Data Protection Officer; it is responsible for informing and advising its staff about their data protection obligations, and for monitoring compliance with those obligations. If you have any questions or comments about the content of this Policy or if you need further information, you should contact the Data Protection Team via email at data-protection@imperial.ac.uk.

Scope

2.1 All staff, students and other authorised third parties (including temporary and agency workers, contractors, casual workers, interns and volunteers) who have access to any personal data held by or on behalf of the university, must adhere to this Policy and associated Codes of Practice.

2.2 Personal data means any information relating to an identified or identifiable natural person (referred to as a 'data subject'); 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.

2.3 The information covered by the Policy includes all written, spoken and electronic personal data held, used or transmitted by or on behalf of the university, in whatever media. This includes personal data held on computer systems, hand-held devices, phones, paper records, and personal data transmitted orally.

2.4 The university will review and update this Policy in accordance with our data protection obligations. The university may amend, update or supplement it from time to time and will issue an appropriate notification of that at the relevant time.

Data Protection Principles

3.1 The university will comply with the following data protection principles when processing personal data:

(a) we will process personal data lawfully, fairly and in a transparent manner;

(b) we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

(c) we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;

(d) we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;

(e) we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and

(f) we will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

3.2 The university is also responsible for demonstrating compliance with the above data protection principles.

Basis for processing personal data

4.1 In relation to any processing activity that involves personal data we will, before the processing starts for the first time, and then regularly while it continues:

4.1.1 Review the purposes of the particular processing activity, and select the most appropriate lawful basis for that processing. For personal data these consist of.:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the university is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority by the university ; or

(f) where the university is not carrying out tasks as a public authority, that the processing is necessary for the purposes of the legitimate interests of the university or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

4.1.2 Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

4.1.3 Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.

4.1.4 Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices.

4.1.5 Where sensitive personal data are processed, also identify a lawful special condition for processing that information (see paragraph 5 below), and document it.

Special category data

5.1 Sensitive personal data (otherwise referred to as 'special category personal data') are 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.

5.2 The university may need to process sensitive personal data. We will only process sensitive personal data if:

5.2.1 We have a lawful basis for doing so as set out in paragraph 4.1 above; and

5.2.2 One of the special conditions for processing sensitive personal data applies, e.g.:

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the university or of the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body;

(e) the processing relates to personal data which are manifestly made public by the data subject;

(f) the processing is necessary for the establishment, exercise or defence of legal claims;

(g) the processing is necessary for reasons of substantial public interest;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care; or

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

5.3 The university's data protection privacy notices set out the types of special category personal data that it processes, what they are used for and the lawful basis for the processing.

5.4 Special category data will be processed in accordance with the university's Special Category Data Policy / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/Special-Category-and-Criminal-Offence-Data.pdf

Records of Processing Activity (RoPA) and Data Protection Impact Assessment (DPIA)

6.1 The university utilises a combined Record of Processing Activity and Data Protection Impact Assessment (DPIA) platform called the Data Asset Registration Tool (DART) which contains details of assets held and involve the processing of personal data. It is the responsibility of Heads of Departments and Divisions to assign Information Asset Owners for every information asset kept by their departments and record these within DART.

6.2 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the university is planning to use a new form of technology), those responsible in the university will, before commencing the data processing, carry out a full DART registration which will encompass the DPIA process. It is the responsibility of the Heads of Departments and Divisions to confirm Information Asset Owners and annually review their Information Assets recorded in DART as described in Code of Practice 5 - 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 and Code of Practice 7 – 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 to consider:

(a) whether the processing is and / or remains necessary and proportionate in relation to its purpose;

(b) the risks to individuals and whether any new risks have been identified; and

(c) what measures can be put in place to address those risks and protect personal / special category data.

Documentation and Records

7.1 Those responsible for processing personal data will keep written records of their processing activities and this will be done primarily within the DART platform. Each information asset will have an identified Information Asset Owner who will be responsible for the information and for logging a description of the processing on the register.

7.2 The university will conduct regular reviews of the personal data we process and update our documentation accordingly. This may include:

(a) carrying out information audits to find out what personal data it holds and ensure this aligns to DART entries and/or create new entries accordingly;

(b) distributing questionnaires and talking to staff to get a more complete picture of our processing activities; and

(c) reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

Privacy Notices

8.1 The university will issue privacy notices informing the people, from whom we collect their personal data, of all relevant and required information including what we collect and hold relating to them, how they can expect their personal data to be used, and for what purposes.

8.2 The university will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Individual Rights

9.1 Data subjects have the following rights, pursuant to any exemptions and derogations, in relation to their personal data, to:

9.1.1 Be informed about how, why and on what basis that data is processed.

9.1.2 Obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a subject access request — see Code of Practice 3 about the procedure.

9.1.3 Have data corrected if it is inaccurate or incomplete.

9.1.4 Have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten').

9.1.5 Restrict the processing of personal data where the accuracy of the information is contested, or the processing is unlawful (but the data subject does not want the data to be erased), or where the university no longer needs the personal data but the data subject requires the data to establish, exercise or defend a legal claim.

9.1.6 Restrict the processing of personal data temporarily where the data subject does not think it is accurate (and the university is verifying whether it is accurate), or where the data subject has objected to the processing (and the university is considering whether the university's legitimate grounds override the data subject's interests).

9.2 Each of the privacy notices provides details of how these individual rights can be exercised. In most cases, individuals are advised to contact the Data Protection Team.

Individual obligations

10.1 Individuals are responsible for helping the university keep their personal data up to date. Individuals should let the university know if the information they have provided changes, e.g. if one moves house or changes details of the bank or building society account into which they are paid.

10.2 Members of staff may have access to the personal data of other members of staff, students and other clients and suppliers in the course of their employment or engagement. If so, the university expects such members of staff to help meet the organisations data protection obligations to those individuals.

10.3 If a staff member has access to university personal data, they must:

10.3.1 Only access the personal data that they have authority to access, and only for authorised purposes.

10.3.2 Only allow others to access personal data if they have appropriate authorisation to do so.

10.3.3 Keep personal data secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Information Security Policy and related Codes of Practice).

10.3.4 Not remove personal data, or devices containing personal data (or which can be used to access it), from university premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device.

10.3.5 Store personal data in line with university standards as described within the Information Security Policy / 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/Information-Security-Policy-v7.0.pdf

10.4 The Data Protection Officer should be contacted if a member of staff is concerned or suspects that one of the following has taken place (or is taking place or likely to take place):

10.4.1 Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal data, without also one of the conditions in paragraph 5.2.2 above being met.

10.4.2 Access to personal data without proper authorisation.

10.4.3 Personal data are not kept or deleted securely.

10.4.4 Removal of personal data, or devices containing personal data (or which can be used to access it), from university premises without appropriate security measures being in place.

10.4.5 Any other breach of this Policy or of any of the data protection principles set out in paragraph 3 above.

Information security

11.1 The university will use appropriate technical and organisational measures in accordance with the Information Security Policy and related Codes of Practice to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Storage and retention

12.1 Personal data (and sensitive personal data) will be kept securely in accordance with the Information Security Policy.

12.2 Personal data (and sensitive personal data) should not be retained for any longer than necessary and as expressed to data subjects. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. The Retention Policy and Schedule (that are maintained by the Archives and Corporate Records Unit) set out the relevant retention period, or the criteria that should be used to determine the retention period – the Retention Schedule is available at:

https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/records-and-archives/public/RetentionSchedule.pdf

12.3 Where there is any uncertainty with respect to data retention, staff should consult the Archives and Corporate Records Unit via email at acru@imperial.ac.uk.

12.4 Personal data (and special category personal data) that are no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data Breaches / Data Incidents

13.1 A data breach may take many different forms, for example:

13.1.1 Loss or theft of data or equipment on which personal data is stored.

13.1.2 Unauthorised access to or use of personal data either by a member of staff or third party.

13.1.3 Loss of data resulting from an equipment or systems (including hardware and software) failure.

13.1.4 Human error, such as accidental deletion or alteration of data.

13.1.5 Unforeseen circumstances, such as a fire or flood.

13.1.6 Deliberate attacks on IT systems, such as hacking, viruses or phishing scams.

13.1.7 'Blagging' offences, where information is obtained by deceiving the organisation which holds it.

13.2 If anyone believes personal data held by the university have been compromised in some way they MUST report this immediately by contacting the Data Protection Team via https://www.imperial.ac.uk/admin-services/governance/policies-and-guidance/data-breaches/.

13.3 The university will:

13.3.1 Investigate any reported actual or suspected data security breach.

13.3.2 Where applicable, make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals.

13.3.3 Notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

International Transfers

14.1 The university may transfer personal data outside the UK to the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway), to other countries on the basis that such countries are designated as having an adequate level of protection or to other third countries.

14.2 When such a transfer occurs, relevant technical and legislative controls will be in place. These will include:

14.2. 1 Inclusion of standard data protection clauses or data sharing schedules.

14.2.2 Inclusion of the UK International Data Transfer Agreement (IDTA) or the EU Standard Contract Clause (EU SCCs) and UK IDTA Addendum.

14.2.4 Creation of a Transfer Risk Assessment.

14.2.5 Capturing explicit consent from data subjects.

14.2.6 Identifying any relevant exception under the legislation.

14.3 We will inform data subjects of any envisaged international transfers in the relevant privacy notice along with the mitigations which are in place.

Training

15.1 Staff need to be adequately trained regarding their data protection responsibilities as per the Imperial Essentials mandatory training packages. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Consequences of failing to comply

16.1 Imperial takes compliance with this policy very seriously. Failure to comply with the policy:

16.1.1 Puts at risk the individuals whose personal data is being processed.

16.1.2 Carries the risk of significant civil and criminal sanctions for the individual and the university.

16.1.3 May, in some circumstances, amount to a criminal offence by the individual.

16.2 Because of the importance of this Policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under the university's procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this Policy, they may have their contract terminated with immediate effect.

16.3 If you have any questions or concerns about anything in this Policy, do not hesitate to contact the Data Protection Officer at dpo@imperial.ac.uk.

Document Control

Document title:		Data Protection Policy	
Version:	4.4	**Date:**	18/12/2025
Initially approved by and date:		Provost January 2013	
Version approved by and date:		University Management Board / 8 December 2025	
Version effective from:		December 2025	
Originator:		Division of the University Secretary	
Contact for queries:		Data Protection Officer	
Cross References:		CoP 01 – Handling of Personal Data CoP 02 – Body Worn Camera CoP 03 – Access to Personal Data CoP 04 – CCTV CoP 05 – Information Asset Register CoP 06 – Internal Sharing and Integration CoP 07 – Data Protection Impact Assessment	
Notes and latest changes:		January 2013 / V1.0 - Approved February – June 2016 / V1.1 - Revised version reviewed by University Secretary and Chief Information Officer July 2016 / V1.2 - Reviewed by IGSG but not published March 2018 / V1.3 - Reviewed by Director of Legal Services April 2018 / V2.0 - Approved by Provost Board March 2019 / V2.1 - Reviewed by Data Protection Officer, Head of Governance (ICT) and Compliance and Information Governance Manager (ICT) April 2019 / V3.0 - Approved by IGSG July 2020 / V3.1 - Reviewed by DPO - DPIA code of practice moved from under Information Security Policy to Data Protection Policy. Contents of Paragraph 5 IAR and DPIA have been inserted under Section 6. January 2021 / V3.2 - 1.1. amended to refer to “the EU or UK-specific version (as applicable)” of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. - V4.0 Approved by IGSG. March 2022 / V4.1 - Updated EU GDPR to UK GDPR. - Update CoP names and remove decommissioned CoP reference. - 5.2 removed language ‘from time to time’. - 6 updated to cite DART and how it will be combining the IAR and DPIA process. - 7. updated to cite DART. - 12.3 amended to reference ACRU as point of contact re retention for ICL data and not the DPO. - 14 amended to reflect the UK is not part of EU anymore.	

	- V4.2 Approved by IGSG. February 2025 (first review not completed) / V4.3 - Updated branding / document template in line with new branding guidelines - Removed all references to 'College' as per branding guidelines. - Updated / corrected all URLs, contact details and references/citations where necessary. - Replaced references to 'sensitive data' with 'Special category data'. - Reference / link to university Special Category Data Policy. - Include references to use of the Data Asset Registration Tool (DART) for recording and completing RoPA and DPIA actions. September 2025 / V4.4 - Updated section 'Data breaches' in line with local procedures. - Removed duplicated information which is covered elsewhere in ICT Security Policy and relevant Codes of Practice. - Added URL's for Data Protection Codes of Practice November 2025 / V4.4 - Proposed changes reviewed by Audit and Risk Committee December 2025 / V4.4 - Approved by University Management Board