DPA CoP 01: Handling of Personal Data

Introduction

1. This Code of Practice, drawn up in association with the Data Protection Policy, relates to the collection, holding and disclosure of data relating to individuals. The CoP provides best practice for staff and students of the university and other authorised persons who collect, process, disclose or have access to personal data in whatever medium that data is held. In the terms of the UK General Data Protection Regulation (GDPR), "processing" covers all aspects of handling personal data, including obtaining, recording, holding, retrieving, collating, disclosure, erasure and destruction of data.

Record of Processing Activities (RoPA)

2.1 Using the Data Activity Risk-assessment Tool (DART) / https://www.imperial.ac.uk/admin-services/secretariat/policies-and-guidance/data-assessments/, the university has an obligation to keep records of its data processing activities, otherwise known as the Records of Processing Activity (ROPA). This replaced the obligation to notify the Information Commissioner of what personal data the university processes. The records must include:

- the contact details of the Data Protection Officer;
- the purposes of the processing;
- the categories of data subjects and personal data processed;
- the categories of recipients with whom the data may be shared;
- information regarding Cross-Border Data Transfers;
- the applicable data retention periods; and
- a description of the security measures implemented in respect of the processed data.

2.2 Upon request, these records must be disclosed to the Information Commissioner.

2.3 To help the university comply with its record keeping obligations, all data assets (that contain personal data) must be registered onto the DART and must have an identified Information Asset Owner who is responsible for the record.

Collection and processing of personal data

3.1 Collection and processing of personal data must comply with the data protection principles.

3.2 Personal data users have a duty to make sure that they comply with data protection legislation and handle personal data in accordance with the data protection principles as set out in the Data Protection Policy. In summary these state that the university will:

- process personal data lawfully, fairly and in a transparent manner;
- 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;
- only process the personal data that is adequate, relevant and necessary for the relevant purposes;
- keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;
- 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;
- 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;
- demonstrate compliance with the above data protection principles.

3.3 Personal data is "any information relating to an identified or identifiable natural person (referred to as a "data subject"); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. So, some obviously personal data are name, contact details (post, phone, e-mail etc.), relationship, educational and financial details. Less obviously personal data are IP addresses and device IDs, pseudonymous data (e.g. hashed or encrypted data).

3.4 In addition, some personal data is identified as 'higher risk' for the data subject known as 'sensitive personal data' or 'special category data'. These are data types relating to a data subject's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of unique identification

- health
- sex life or sexual orientation

3.5 Sensitive personal data has a higher standard of protection than other personal data.

3.6 Data protection legislation also treats criminal data with a higher degree of care than other personal data.

3.7 The term "processing" is very broad. It essentially means anything that is done to, or with, personal data (including simply collecting, storing or deleting those data). This definition is significant because it clarifies the fact that the UK GDPR is likely to apply wherever an organisation does anything that involves or affects personal data.

Processing personal data

4.1 The university processes personal data under one of six prescribed lawful basis. Seeking consent from the individuals whose data they are is one basis for processing but should be considered only where there is no more suitable legal basis for the processing.

4.2 The six lawful basis for processing personal data are:

- processing is permitted if it is necessary for the entry into, or performance of, a contract with the data subject or in order to take steps at his or her request prior to the entry into a contract (in short, there is contractual necessity);
- processing is permitted if it is necessary for compliance with a legal obligation (in short, where the university has to comply with a UK or international law);
- processing is permitted if it is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is permitted if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (in short, this would be relevant for some functions carried on by the university such as teaching and research in the public interest);
- processing is permitted if it is necessary for the purposes of legitimate interests pursued by the controller (or by a third party), except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects which require protection, particularly where the data subject is a child.

  This does not apply to processing carried out by public authorities in the performance of their duties i.e. the university cannot rely on this basis with respect to activities that are carried out in the public interest such as teaching and research in the public interest;
- processing is permitted if the data subject has consented to the processing.

4.3 Consent must be unambiguous, verifiable (including proof of consent), distinguishable from other matters, easy to withdraw and generally must not be conditioned on access to a service. Silence, inactivity and pre-ticked boxes do not amount to consent. If we seek consent to the processing of personal data, individuals will be able to exercise the right to erasure, right to object and the right to portability more easily.

Processing special category data

5.1 The UK GDPR imposes a number of additional restrictions and conditions on data controllers who want to record and process special category personal data. The university can process sensitive personal data when, in addition to having a lawful basis for personal data (as explained above), we can also satisfy at least one of the following ten legal basis:

- legal claims
- it is necessary in the context of employment law, or laws relating to social security and social protection
- reasons of substantial public interest
- to protect vital interests
- medical diagnosis and treatment (undertaken by health professionals, including assessing the working capacity of employees)
- charity or not-for-profit bodies with respect to their own members
- public health
- data manifestly made public by the data subject
- for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards
- explicit consent

5.2 Most personal data which is collected on a day-to-day basis will be for general administrative purposes, and will cover categories such as:

- general personal details such as name, address, date of birth and next of kin;
- details about class attendance, course-work marks and grades and associated comments;
- notes of personal supervision, including matters about behaviour and discipline;
- management of student clubs and societies.

5.3 A data protection impact assessment (DPIA), must be conducted:

- where there is "high risk" to data subject rights and freedoms;
- prior to processing occurring
- in consultation with the Data Protection Office.

5.4 A DPIA is always required where there will be:

- automated decision with legal / significant effect;
- processing of special category data;
- large scale data processing;
- large scale monitoring of public areas.

5.5 Consultation with the Information Commissioner's Office is required if high risk cannot be mitigated.

5.6 The university has an online platform for recording DPIA's called the Data Asset Registration Tool (DART). See Data Protection Code of Practice 5 Information Asset Register for more information.

5.7 Data Subjects must be informed of the purposes for which data are being collected at the point of collection. The university informs students and prospective students of how it uses their personal data in its Privacy Notice for Students and Prospective Students / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/registry/academic-governance/public/academic-policy/admissions/Privacy-notice.pdf, staff and prospective staff in its Privacy Notice for Staff and Prospective Staff / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/public/data-protection/Privacy-Notice-for-Staff-and-Prospective-Staff.pdf and alumni and supporters in the Privacy Notice for Advancement / https://www.imperial.ac.uk/admin-services/advancement/about-us/advancement-policies/privacy-policy/. Any additional processing which is done and which is not explained and provided for in these notices or which applies to other categories of Data Subjects will require careful analysis as to the lawful basis of processing, potentially the completion of a data protection impact assessment and have its own privacy notice to inform the relevant Data Subjects of the proposed processing.

5.8 All personal data must be held securely in accordance with 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. All persons having access to such data shall treat it as confidential and shall not communicate it to other persons or bodies except in accordance with this Code of Practice.

5.9 Before processing any personal data, members of the university and other authorised individuals should study the checklist for processing data set out in the Appendix to this Code.

5.10 Where any of the data protection principles are not followed data users may find themselves subject to university disciplinary procedures. Also, the university may be investigated and fined by the Information Commissioner's Office and may be liable to pay compensation to any affected individuals.

Disclosure of personal data to third parties

6.1 No data relating to a particular student, member of staff or other individual acquired in the course of an individual's duties should be disclosed to anyone (including other students or staff) unless:

- required for normal academic, administrative or pastoral purposes of university business, or
- the individual concerned has given permission, or
- it is required as part of the discharge of regulatory functions or required by legislation, or
- in the case where, even though prior consent has not been given, disclosure is deemed to be needed to protect the vital interests of the individual, or it is required for the prevention or detection of crime, or the apprehension or prosecution of offenders, or
- in certain limited cases and subject to certain conditions and safeguards, it is used for other legitimate purposes.

6.2 In many cases, sharing of personal data occurs when the university appoints another organisation to process data that belongs to it on behalf of the university, where an organisation provides services that require access to university-owned personal data or to systems holding university-owned personal data. This is known as appointing a data processor.

6.3 The university must only use data processors that guarantee compliance with the UK GDPR. To do this the university must have documented what the data processor will be doing, in the form of a binding agreement (such as a data processing agreement or a services agreement with appropriate data processing clauses included), which states that the processor must only act on the university's documented instructions. The agreement must also contain a number of other provisions prescribed by the UK GDPR. The university has a data processing agreement template suitable when such a situation occurs. Please contact the relevant contracts team or DPO for a suitable template.

6.4 Before sharing any data (personal or other) staff should consider the following key questions:

- do you have the legal power or ability to share the data in question?
- will the proposed data sharing involve sharing of "standard" personal data and/or sensitive personal data and, if so, would the sharing be fair, transparent and in line with the rights and expectations of the people whose information is being shared?
- is there any specific statutory prohibition on sharing the data in question?

- are there any copyright restrictions?
- is there a duty of confidence (express or implied by the content of the information or because it was collected in circumstances where confidentiality was expected e.g. medical or banking information)?
- if a decision is ultimately taken to share data with another organisation or person, will a data processing or data sharing agreement be signed or will the services agreement include data processing/sharing provisions? Having data processing clauses (in the case of using a data processor) are mandatory requirements under the legislation.

Transfer of data overseas

7.1 The transfer of personal data to recipients outside the UK is generally prohibited unless:

- the jurisdiction in which the recipient is located is deemed to provide an adequate level of data protection;
- the data exporter puts in place appropriate safeguards, such as including the UK International Data Transfer Agreement (IDTA); or
- a derogation or exemption applies such as the transfer is required for the performance of a contract between a data subject and a data controller, or for taking steps at the request of a data subject with a view to entering into such a contract, or where specific and informed consent of the data subject has been obtained for effecting such a transfer.

7.2 Where staff contemplate transferring personal data outside the UK, they should discuss the proposal with the relevant contract team, Faculty IG lead or Data Protection Office to establish if there is a lawful mechanism for such a transfer.

7.3 Subject to taking appropriate security measures, as set out in section 8, personal data may be transferred to and from countries in the European Economic Area (EEA) without further restriction.

7.4 Proper records must be kept justifying any decision made about such exempted transfers, or clear evidence can be demonstrated showing the Data Subject had given consent to the transfer, having been suitably informed.

7.5 In the absence of a sponsorship arrangement between the university and an external body in respect of a particular student, personal data should not be disclosed in response to a request from non-EEA governments, agencies or organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas without specific informed consent of the Data Subject(s) concerned, nor should such data be disclosed to such bodies for the purposes of determining liability to attend National Service without such consent.

Security

8.1 Proper security measures must be applied to all methods of holding or displaying personal data and appropriate measures taken to prevent loss, destruction or corruption of data. For fuller details on security measures see the Information Security Policy, Information Governance Framework and associated Codes of Practice.

8.2 Staff, students and authorised third parties are not permitted to remove from the university personal data with the intention of processing this information elsewhere, unless such use is authorised by the data owner and that authorisation recorded. Removing data in this way must not compromise the standards of security operating within the university, and the data protection principles should be observed at all times.

APPENDIX - Checklist for processing of personal data

Lawfulness

- We have identified an appropriate lawful basis for our processing.
- If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.
- We don't do anything generally unlawful with personal data.

Fairness

- We have considered how the processing may affect the individuals concerned and can justify any adverse impact.
- We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.
- We do not deceive or mislead people when we collect their personal data.
- If yes, are there mechanisms in place to check the accuracy of the data?

Transparency

- We are open and honest, and comply with the transparency obligations of the right to be informed.

Assessment / RoPA

- Has a data protection impact assessment been carried out either because it is mandatory or as best practice? If not see Data Activity Risk-assessment Tool – DART / https://www.imperial.ac.uk/admin-services/secretariat/policies-and-guidance/data-assessments/
- Has the activity been recorded centrally as an activity? If not see Data Activity Risk-assessment Tool – DART / https://www.imperial.ac.uk/admin-services/secretariat/policies-and-guidance/data-assessments/.

Document Control

Document title:		DPA CoP 01: Handling of Personal Data	
Version:	2.1	**Date:**	November 2025
Initially approved by and date:		Provost Board / May 2018	
Version approved by and date:		Data Protection Officer / November 2025	
Version effective from:		November 2025	
Originator:		Division of the University Secretary	
Contact for queries:		Data Protection Officer	
Cross References:		Data Protection Policy / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Data-Protection-Policy.docx 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 Information Governance Policy Framework / https://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/secretariat/public/information-governance/Information-Governance-Policy-Framework---to-be-reviewed.pdf	
Notes and latest changes:		May 2018 V1.0 - Approved by Provost Board March 2021 V1.1 - No changes March 2022 V.2 - Throughout - amended to reference DART - Throughout - amended to reference UK / international legislation as opposed to EU legislation only - Section 1.20 Updated links to Staff / Student / Advancement Privacy Notices - Section 1.24.4 reference contract teams as primary contact relating to onboarding of data processor agreements - Section 1.25.2 reference contract teams and Faculty IG leads for support April 2022 V1.2 - Approved February 2025 V2.0 - Updated to meet new brand standard - Removal of references to 'College' - Amended / replaced all references to the term 'College' - Shortened sentences where appropriate - Corrected terminologies to align across all documentation - Removed 1.25.2 as not necessary - Updated URL for Data Asset Registration Tool, Staff Privacy Notice and Student Privacy notice - Updated Questionnaire November 2025 V2.1 - Amended name of DART - Corrected broken URL for the Student Privacy Notice - Removed hidden URL's for purpose of improving accessibility.	