Imperial College
London

Imperial College

Data Protection Code of Practice 1: Handling of Personal Data

Doc. Ref.	: Data Protection Code of Practice 1: Handling of Personal Data
Version	: 1.1
Status	: Approved
Date	: 06/04/2022
Approved by	: The Information Governance Steering Group
Review by	: 30/04/2024

INTRODUCTION

1.1 This Code of Practice, drawn up in association with the College's Data Protection Policy, relates to the collection, holding and disclosure of data relating to individuals. The Code provides best practice for staff and students of the College 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 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.

KEEPING RECORDS OF PROCESSING ACTIVITIES

1.2 Via the Data Asset Registration Tool Platform, see Data Asset Registration Tool - DART, the College has an obligation to keep records of its data processing activities, otherwise known as the Information Asset Register or Records of Processing Activity (ROPA). This replaced the obligation to notify the Information Commissioner of what personal data the College processes. The records that the College must keep include:

- the contact details of the College/its representative (if applicable)/ 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.

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

1.4 To help the College comply with its record keeping obligations, all College information assets (including those that contain personal data) must be registered into the College's Data Asset Registration Tool (DART) and must have an identified Information Asset Owner who (among other things) is responsible for updating the record as and when necessary.

COLLECTION AND PROCESSING OF PERSONAL DATA

1.5 Collection and processing of Personal Data must comply with the data protection principles.

1.6 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 College Data Protection Policy. In summary these state that the

College 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.

1.7 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).

1.8 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

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

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

1.11 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 GDPR is likely to apply wherever an organisation does anything that involves or affects personal data.

1.12 Processing personal data

1.12.1 The College, processes personal data under one of six prescribed lawful basis for processing personal data. 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.

1.12.2 The six lawful basis 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 College has to comply with a UK or EU 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 College 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 College 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.

1.12.3 Consent must be unambiguous, verifiable (we ought to document proof of consent), distinguishable from other matters, easy to withdraw, (generally) must not be conditioned on access to a service. Silence, inactivity and pre-ticked boxes do not amount to consent.

1.12.4 Not only that the standard of valid consent under the GDPR is high but also if we seek consent to the processing of personal data, the individuals who have consented will also be able to exercise the right to erasure and the right to portability more easily.

1.13 Processing sensitive data

1.13.1 The GDPR imposes a number of additional restrictions and conditions on data controllers who want to record and process sensitive personal data. The College can process sensitive personal data when, in addition to having a lawful basis for personal data as explained above, we can also satisfy one of ten additional grounds, which are as follows:

- 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

1.14 Staff, and students, collect both 'personal' and 'sensitive personal data' on employees, students and other individuals.

1.15 Most personal data which is collected on a day-to-day basis will be 'personal', i.e. 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.

1.16 A data protection impact assessment (in short, DPIA), must be conducted:

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

1.17 A DPIA is always required where there will be:

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

1.18 Consultation with the Information Commissioner is required if high risk cannot be

mitigated.

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

1.20 Data Subjects must be informed of the purposes for which data are being collected at the point of collection. The College informs students and prospective students of how it uses their personal data in its Privacy Notice for Students and Prospective Students [PDF], staff and prospective staff in its Privacy Notice for Staff and Prospective Staff [PDF] and alumni and supporters in the Advancement Privacy Notice [PDF]. 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, data protection impact assessment and have its own privacy notice to inform the relevant Data Subjects of the proposed processing.

1.21 All personal data must be held securely in accordance with the College's Information Security Policy. 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.

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

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

1.24 Disclosure of personal data to third parties

1.24.1 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 College business, or
- the individual concerned has given permission, or
- they are required to do so in 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 Data Subject or itis 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 legitimate purposes.

1.24.2 In many cases, where sharing of personal data is relevant to College is where College appoints another organisation to process data that belongs to the College on behalf of the College or where an organisation provides services to the College that require that organisation to have access to College-owned personal data or to systems holding College-owned personal data. This is

known as appointing a data processor.

1.24.3 The College must only use data processors that guarantee compliance with the GDPR. The College must appoint the data processor in the form of a binding agreement in writing (such as a data processing agreement or a services agreement with appropriate data processing clauses), which states that the processor must only act on the College's documented instructions. The agreement must also contain a number of other provisions prescribed by the GDPR. The College has a data processing agreement template suitable when the College engages processors based in the UK / EEA. For any other data processing arrangements, staff should contact the relevant contracts team or DPO for a suitable template.

1.24.4 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 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? Check what people have been told in the relevant privacy notice about data sharing.
- 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)?

1.24.5 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? This is a requirement.

1.25 Transfer of data overseas

1.25.1 The transfer of personal data to recipients outside the UK/EEA 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; 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.

1.25.2 Where staff contemplate transferring personal data outside the UK/EEA, 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.

1.25.3 Posting personal data to the World Wide Web constitutes transfer of data worldwide. A third party accessing College-owned personal data from outside the UK/EEA would also constitute a transfer of data outside the UK/EEA. Using a cloud services provider with servers outside the UK/EEA would also constitute a transfer of data outside the UK/EEA. However, if data is only in transit through a non-UK/EEA country (and is not accessible) this will not constitute a transfer outside the UK/EEA.

1.25.4 Subject to taking appropriate security measures, as set out in 3.22 below, personal data may be transferred to and from countries in the European Economic Area (EEA) without further restriction.

1.25.5 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.

1.25.6 In the absence of a sponsorship arrangement between the College 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.

1.26 Security

1.26.1 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 College Information Security Policies, associated Codes of Practice and Guidelines.

1.26.2 Staff, students and authorised third parties are not permitted to remove from the College 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 College, and the data protection principles should be observed at all times.

APPENDIX - CHECKLIST FOR PROCESSING OF PERSONAL DATA

- Do you really need to record the information?
- Which is your legal basis for processing the information (one of six basis)?
- Is the information "standard" or is it "sensitive"?
- If it is sensitive information, do you satisfy one of the ten additional conditions to be able to process the information?
- If you are going to rely on consent to process “standard” personal data or “sensitive” personal data, are you able to obtain valid consent?
- Has the data subject been told how the data will be processed?
- Are you authorised within College to collect/store/process the data?
- If yes, are there mechanisms in place to check the accuracy of the data?
- Is it clear who else has a right to access/process these data?
- Do you have mechanisms in place to ensure that the data are kept securely whether held electronically or in a relevant filing system?
- Are you clear as to how long you may retain these data? Have you checked the College’s Retention Schedule to see if it prescribes any retention period for these data?
- Do you have procedures in place to ensure that the data are kept up to date?
- Do you have procedures in place to remove these data securely when it is no longer needed?
- Do you have procedures in place to remove these data where a data subject exercises their right for it not to be processed;
- Has a data protection impact assessment been carried out either because it is mandatory or as best practice?

Version History

Version/Status	Release Date	Comments
1.0/Approved	May 2018	Approved
1.1/In Review	March 2021	No changes
1.1/In Review	March 2022	• Throughout - amended to reference DART • Throughout - amended to reference UK / EU 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
1.1/In Review	April 2022	Approved