Imperial College London

Data Protection Team

Complaint Plan / SOP

Author	Robert J Scott
Review Date	January 2027
Version	1.5

1. Introduction

1.1. The UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), and the Privacy and Electronic Communications Regulations ("PECR") (together, the "Data Protection Legislation"), give data subjects and applicable third parties rights in relation to personal data. This procedure details how the University will respond to complaints from data subjects and third parties relating to the use of personal data

Who are Data Subjects?

1.2. Data subjects are any natural living individuals whose personal data Imperial could process (collects, obtains, stores, retains, disposes of etc.). Data subjects can include staff members, students, applicants, prospective applicants, alumni, visitors, representatives, individuals captured by the University's CCTV cameras, etc.

Data subjects' rights under legislation

1.3. Under Data Protection legislation, data subjects have the right to the following and these rights can be exercised at any time:

a. information about the processing of their data (UK GDPR Articles 12-14, and Recitals 58-62), b. access their own personal data (UK GDPR Articles 12 and 15, and Recital 63),

c. correct personal data (UK GDPR Article16),

d. erase personal data, also known as the right to be forgotten (UK GDPR Article 17, and Recitals 65 and 66),

e. restrict data processing (UK GDPR Article 18),

f. object to data processing, including direct marketing (UK GDPR Article 21, and Recitals 69 and 70),

g. receive a copy of their personal data or transfer their personal data to another data controller (data portability, UK GDPR Article 20, and Recital 68),

h. not be subject to automated decision-making and rights in relation to profiling (UK GDPR Article 22, and Recital 71), and

i. be notified of a data security breach (UK GDPR Article 34, and Recital 86).

What is a complaint?

1.4. A complaint is an expression of dissatisfaction about the University's handling of a data subject's personal data. This can also include dissatisfaction with how the University has responded to a previous data request, such as those detailed under 1.3.

2. Scope

2.1. This procedure addresses complaints made by data subjects regarding the use of their personal data. Complaints may be made in relation to any aspect of the University's processing of personal data including individual rights requests.

2.2. This procedure also addresses complaints made by third parties in relation to the University's use of personal data. These may be for example in relation to the University's

response to a data related request from a third party, such as the Police or Local Government Agencies.

2.3. This procedure should also be followed for complaints in relation to use of personal data for direct marketing and/or profiling activity.

3. Responsibilities

3.1 The Data Protection Officer / Deputy Data Protection Officer and Access to Information Manager will review this procedure from time to time (and at least every two years) to ensure that its provisions continue to meet our legal obligations and reflect best practice.

4. Making a Complaint

4.1. Complaints should be sent directly to the Data Protection Officer at data-protection@imperial.ac.uk or to subjectaccess@imperial.ac.uk, if it relates to a subject access request. The university will aim to acknowledge receipt of the complaint within 5 working days. The University reserves the right to extend the period we need for response, but will aim to respond within 28 days.

4.2 Complaints received elsewhere within the university, by other members of staff, should be forwarded to the Data Protection Officer as soon as possible to avoid delay.

4.3. Although a complaint may be brought at any time, there may be limits as to what the University can do in historic cases.

4.4. The University will only accept a complaint from a data subject's representative, if the university has received the data subject's written consent authorising the representative to act on the data subject's behalf in relation to the complaint.

4.5 If there is any doubt about the identity of the complainant the receiving team will first seek to verify the data subject's identity or third party's entitlement to act on behalf of the individual. The forms of identification that are acceptable from a data subject are as follows;

a. Passport
b. Government ID Card
c. College ID Cards
d. Driving Licence
e. For third parties the identification requirements will vary dependent on their relationship to the data subject. Therefore, these will be assessed on a case-by-case basis.

Once identification is confirmed the form of identification should be erased unless there is a reason for retention and this is explained to the data subject.

5. Investigation and Complaint Outcome

5.1. Once all identification requirements have been met, the investigation will be carried out normally within 28 days. If further clarification is required from the complainant or more time is required for the response to be completed, the University will inform the complainant prior to the original deadline.

5.2. The investigating team will carry out the complaint investigation as necessary to answer the issues raised. This may involve speaking with other individuals named or involved with the

situation, engaging with third party organisations and / or requesting access to any documentation / information they feel pertinent.

5.3. The processing of any and all personal data as part of the complaint, once received, will not require the prior consent of any individual involved to be obtained.

5.4. Should the complaint investigation interact or overlap with any other University process these will be managed between the investigating team and relevant department to ensure the complaint investigation does not stifle or delay any other University procedure.

5.5. The complaint outcome will be communicated to the complainant in writing, normally by email and further options presented, such as an internal review or raising a concern to the Information Commissioners Office.

6. Review

6.1. If the complainant does not agree with the outcome, they can request a review of the decision. This request must be made within 1 month of the original decision being communicated and should be sent to the investigating team via data-protection@imperial.ac.uk or subjectacccess@imperial.ac.uk respectively . The decision will then be internally reviewed by a suitable member of staff.

6.2. Once the internal review has been completed, the University will communicate the outcome in writing, normally by email.

7. Information Commissioner's Office

7.1. If the complainant remains dissatisfied, they can escalate their complaint to the Information Commissioner's Office (the "ICO"). Information about how to make a complaint to the ICO can be found here: www.ico.org.uk. The ICO will decide whether to investigate further and will contact the University should they have questions / queries re any actions previously undertaken.

7.2. Once a complaint has been received from the ICO, the Data Protection Officer or Information Compliance Manager – Access and Records will investigate the complaint based on the information provided by the ICO. This may;

a. necessitate access to personal data and other information held across Imperial.

b. Require the cooperation of additional staff members to assist with the investigation where pertinent.

c. require the disclosure of the complaint and its particulars to other related staff members / personnel on a case by case basis.

7.3. The Data Protection Officer or Information Compliance Manager – Access and Records will draft and submit a response to the ICO in consultation with the division leads.

7.4. In the absence of the Data Protection Officer, the Deputy Data Protection Officer will manage the ICO response or the University will appoint another suitable member of staff.

8. Manifestly unfounded, abusive, vexatious or excessive correspondence and complaints Independent External Review

8.1. In some scenarios we can refuse to handle the complaint. This will be when a complaint is deemed to be manifestly unfounded, abusive, vexatious or excessive. Each complaint will be considered on a case by case basis. The following factors will be taken into consideration:

a. the data subject has explicitly stated that they intend to cause disruption (whether in the complaint, or in other correspondence), and has threatened individuals;

b. the data subject has made unsubstantiated accusations against individuals, and is persisting in those accusations;

c. the data subject is targeting particular individuals, against whom they have a personal grudge;

d. the data subject makes frequent complaints intended to cause disruption; and

e. the data subject continues to repeat the substance of previous complaints which have already been investigated.

8.2. Where a complaint is deemed to be manifestly unfounded, excessive, abusive or vexatious the University will contact the individual and in a reasonable timeframe explain to them:

a. the reasons for refusing to consider the complaint;

b. their right to make a complaint to the ICO; and

c. their right to pursue their data subject rights through a judicial remedy.

9. Use of Data from Complaints

9.1. The University will collect data on complaint outcomes at each stage of this procedure and any complaints submitted by complainants to any regulators (including the ICO), and use the data:

a) internally for reporting, evaluation, learning and training; and

b) externally for discussion with regulators

9.2. The data used by the University for the purposes set out in paragraphs 9.1 a) and b) will be anonymised.

9.3. Personal data and sensitive personal data ('Personal Data') as defined by the Data Protection Act 2018 (the "DPA") relating to the complainant and/or staff involved may be disclosed to the University's members of staff and regulators only for the purpose of dealing with the complaint, or a complaint arising out of it and/or implementing any recommendations. Personal Data will not be shared with any other third parties unless the University has gained express consent from the data subject, has a statutory obligation to do so, or is otherwise permitted to do so under the DPA.

9.4. Data / details relating to the complaint will be retained for 6 years, in line with the university Retention Schedule whereby following this time all identifiable data will be erased.