Data Protection Complaints Policy and Procedure

1. Background

1.1 The processing of personal data in the United Kingdom is regulated by law. The principal legislation is the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (GDPR), the Data (Use and Access Act) 2025 (DUAA), the Privacy and Electronic Communications Regulations (2003) and the Freedom of Information Act (2000). These laws are collectively referred to in this policy as data protection legislation.

1.2 The experience of our students and colleagues is of paramount importance to us, and we are committed to the compliant processing of personal data. However, if an individual ever feels that our processing of personal data falls short of the requirements of data protection legislation this policy and procedure details how best to raise and resolve issues.

1.3 We aim to ensure that data protection complaints are treated seriously and dealt with promptly, fairly, impartially and consistently across the University. We also aim to learn from the outcomes of complaints investigations to help us improve our compliance.

1.4 The Data (Use and Access) Act introduces a statutory requirement for all organisations to implement a formal data protection complaints procedure.

1.5 For the purposes of this policy and procedure a Data Protection Complaint is defined as any expression of dissatisfaction by an individual who believes the University has infringed data protection legislation regarding the handling of their personal data.

1.6 A data protection complaint might arise from:

- a data breach which has impacted an individual
- dissatisfaction with the university's response to a privacy rights request
- inappropriate handling of personal data
- handling of personal data which is not in accordance with the principles of data protection legislation
- non-compliant conduct of a processor that the University has appointed

1.7 This policy should be read in conjunction with the University's Data Protection Policy.

2. Scope

2.1 This policy covers all data protection complaints received by the University of Westminster.

3. Data (Use and Access) Act - Section 103

3.1. We will manage data protection complaints confidentially and in compliance with section 103 of the DUAA.

3.2. We will:

- provide a complaint form which can be completed electronically and by other means

- acknowledge receipt of complaints within a period of 15 days beginning when the complaint is received
- take appropriate steps to investigate the complaint to the extent appropriate and without undue delay
- respond to the complaint and inform the complainant of the outcome of the complaint.

3.3 DUAA section 103 is available here: https://www.legislation.gov.uk/ukpga/2025/18/section/103/enacted

3.4 The Information Commission's Guidance is available here: https://ico.org.uk/about-the-ico/what-we-do/complaints-guidance-for-organisations/

4 Data Protection Complaints in Practice

4.1 Raising a Complaint and Acknowledgement

4.1.1 You can raise a data protection complaint using one of the options below:

- completing our data protection complaints form published on our website
- writing to DPA@westminster.ac.uk
- posting your complaint to the following address: Information Compliance Team, University of Westminster, 3rd floor, 32-38 Wells Street, London, W1T 3UW

4.1.2 We will treat complaints seriously and sensitively with proper investigation, proportionate to the issues raised.

4.1.3 You are expected to clearly state the nature and circumstances of your complaint and the remedy you are seeking.

4.1.4 You should raise your complaint at the earliest opportunity and within three months of the occurrence of the matter the complaint is about or within three months of you being notified of a data breach.

4.1.5 Upon receiving a complaint, we will check the details of the complaint and may request further information. It is important that you provide as much information as possible when you raise your complaint.

4.1.6 In some cases, we may request proof of identity.

4.1.7 You can make a complaint on behalf of another person e.g. if you are a solicitor, a family member or another organisation. If you are raising a complaint on behalf of someone else, you must provide a signed letter of authority (or equivalent documentation) before we can investigate the complaint. By providing the letter of authority the complainant gives the University permission to share information relevant to the complaint with their representative. A complainant may revoke representation at any time and must inform the Information Compliance Team in writing as soon as possible.

4.1.8 Complaints should not be false, frivolous, vexatious or malicious. We may not investigate complaints of this nature.

4.1.9 Complaints and communications should not be abusive, offensive, defamatory, aggressive, threatening, coercive or intimidating in manner. We may not investigate complaints of this nature.

4.1.10 We do not accept complaints made anonymously.

4.1.11 Complaints relating to other policies or other regulatory matters will not be addressed under this policy and procedure. Where relevant we will direct you to the appropriate University department or signpost the relevant policy.

4.2 Timescales

4.2.1 We will write to you to acknowledge receipt of the complaint. We aim to do this within 10 days, but at busy times this might take up to 15 days.

4.2.2 The length of time we require to consider a complaint will be dependent on the nature and complexity of the complaint. We aim to respond to complaints within one month (from the date you make your complaint) but complex complaints may take up to three months. We will inform you if we consider your complaint to be complex.

4.3 Investigation

4.3.1 We will investigate each complaint individually. We will determine the most appropriate way in which to undertake the investigation considering the nature, seriousness and sensitivity of the complaint.

4.3.2 Our investigation activities may include (but are not limited to) gathering evidence, meeting with individuals (such as University colleagues or third parties outside of the University), reviewing footage, examining logs, calling for documents, and reviewing the evidence you provide.

4.3.3 Our investigation will be limited to compliance with the legislation outlined in paragraph 1.1 above.

4.3.4 We may share information or evidence relating to a complaint and/or its outcomes with others where we deem such disclosure is appropriate.

4.4 Keeping You Updated

4.4.1 We will communicate with you using the same method you used to raise your complaint unless an alternative has been specifically requested e.g. we will respond by email to complaints received via email.

4.4.2 We will contact you to acknowledge and respond to your complaint, to request clarification or additional information and to notify you about timescales for the investigation.

4.5 Recording Actions

4.5.1 We will log all data protection complaints.

4.5.2 The log will include (as a minimum) your name and contact details, the type of complaint, the date we received the complaint, the outcome and the date we responded to the complaint.

4.5.3 We will monitor complaints to identify any themes, trends or insights that may help us to improve our personal data protection processing practices and procedures.

4.5.4 We will keep records of data protection complaints for three years from the date we close the complaint.

4.6 Informing You of the Outcome of your Complaint

4.6.1 When we conclude our investigation of the complaint, we will inform you in writing of the outcome. Our outcome letter will include details of the investigation, our decision and clear reasons for that decision, and any remedial actions arising from that decision.

4.6.2 Possible outcomes are:

- **Complaint not upheld** - we have fully complied with the requirements of data protection legislation
- **Complaint upheld in part** - we have partially failed to comply with the requirements of data protection legislation
- **Complaint upheld** - we have wholly failed to comply with the requirements of data protection legislation

4.7 If You Remain Dissatisfied

4.7.1 If you disagree with the outcome of our investigation or otherwise remain dissatisfied, you can request a review.

4.7.2 You must submit your request for a review within one month of the date that we sent the initial outcome response to you. We will write to you to confirm receipt of the request for review. We aim to do this within 10 days, but at busy times this might take up to 15 days.

4.7.3 We aim to inform you of the outcome of the review within one month of the date we received it.

4.7.4 Our Senior Information Risk Owner (SIRO) or their nominee will consider all reviews.

4.7.5 Possible outcomes of the review are:

- **Decision upheld** - we uphold our original outcome
- **Decision upheld in part** - we partially uphold our original outcome
- **Decision not upheld** – our review identifies a different outcome from the original outcome

4.7.6 After a review, if you remain dissatisfied with the outcome, you have the right to refer the matter to the regulator - the Information Commission. We will provide details of how to contact the Information Commission on our website and in the review outcome letter.

4.7.7 Please note that you must have exhausted all stages of this complaints procedure for the Information Commission to review your complaint.

4.7.8 We will co-operate with any enquiries or investigations the Information Commission wishes to make.

5 Further Action and Reporting

5.1 When investigating complaints, we may identify further actions that we need to take including:

- updating or refreshing our policies, procedures or practices to prevent future complaints of a similar nature;
- providing additional training for our colleagues; and/or
- reporting the complaint to the Information Commission.

5.2 We will report the number of data protection complaints we receive, resolve and escalate to the regulator to the Information Governance Advisory Group (IGAG) on a termly basis.

6 Policy Roles and Responsibilities

6.1 The Information Compliance Team (managed by the Information Compliance Manager/Data

Protection Officer) and reporting to the Head of University Governance are responsible for:

- maintaining this policy
- managing, logging, handling and responding to data protection complaints
- providing data protection training and support to University colleagues.

7 Wider Roles and Responsibilities

7.1 Directors of Professional Services and other directorates, Heads of Colleges, Heads of Schools and other Heads of Business Units are responsible for ensuring general awareness and compliance with this policy in their areas. The Information Compliance Team can provide specific training and support on request.

7.2 All colleagues must notify the Information Compliance Team if they receive a data protection related complaint.

7.3 All colleagues are responsible for assisting the Information Compliance Team in responding to data protection complaints.

8 Policy review

8.1 The Information Compliance Manager will review this policy annually in collaboration with relevant stakeholders and IGAG.

8.2 The policy is subject to the approval of the University Secretary and Chief Operating Officer/SIRO on the recommendation of IGAG.

9 Digital accessibility

9.1 We are committed to ensuring our websites and content is digitally accessible according to the Public Sector Bodies Accessibility Regulations (2018). This policy is published on our website; and can be requested in a range of formats e.g. Word, PDF, plain text, alternative formats such as large print or Braille.

10 Version record

Version	Date	Author	Description
0.1	March 2026	Information Compliance Manager	Draft – first version
1.0	June 2026	Information Compliance Manager	Final Approved by IGAG and COO (May 2026)