Lancaster University – Data Protection Complaint Process

Document Status	**FINAL**
Document Owner	Information Governance Manager
Target Audience	All Data Subjects
Review Period	3 years
Date of First Approval	April 2026
Date of Next Review	2029
Version Number	V1.0

1. Introduction

1.1 This document sets out the University's Data Protection Complaint Process. Advice on this procedure can be sought from the University's Information Governance Team.

2. Scope

2.1 This Complaint Process will cover any complaint which concerns the use, access, security, or disclosure of personal data by the University. Complaints will be received where they concern any processing of personal data which is subject to UK data protection legislation, i.e. the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), and the Privacy and Electronic Marketing Regulations 2004 (PECR). It will not cover any complaints made under the Freedom of Information Act 2000 (FOIA) or the Environmental Information Regulations (EIR), save for when these complaints relate to the unlawful disclosure of personal data. It will also not apply where an individual has acknowledged that the University responded to their subject access request within one calendar month but expresses dissatisfaction that their request wasn't expedited. Complaints received where the substance of the complaint is about a University service or other matter, whilst also exercising their data subject rights, will not be handled under this Process. For example, where a member of staff raises a grievance issue and also requests a copy of their personal data or where an individual complains about a customer service issue and also requests deletion of their personal data.

2.2 Complaints relating to FOIA and/or EIR will be dealt with in line with the University's established internal review process.

2.3 Only complaints which relate to personal data processed by services offered directly by the University will be considered. Complaints related to third party service providers on campus such as commercial tenants, should be taken up directly with the provider or via the University's Commercial Services. For the avoidance of doubt this includes personal data processed solely by the Students' Union.

2.4 Where it is unclear whether an individual is making a data protection complaint, the Information Governance Team will contact them to clarify the issues they are complaining about and to determine whether the complaint concerns data protection matters.

2.5 Where the complaint relates to a third-party system/service provided to the University as a data processor, the University's Data Protection Officer (or nominated deputy) will liaise with the system/software/service provider to investigate the complaint.

2.6 Where the complaint relates to personal data for which the University is a data processor, the Information Governance Team will direct the complainant to the relevant Data Controller.

2.7 Complaints can be received by emailing the information-governance@lancaster.ac.uk email address or by contacting the University's Data Protection Officer directly.

2.8 Complaints can also be received via the University's official social media accounts. Where a complaint is received on social media, the complainant should be asked for an alternative contact method in order to progress the complaint under this process. Responding on social media is not a secure way of providing information.

2.9 Individuals will be invited to use the online complaint form to submit their complaint but complaints will be received and accepted in whatever format/channel they are received by the University.

2.10 Should the University be required to contact individuals where their personal data has been involved in a personal data breach, a link to the Data Protection Complaints form will be included in any such communication.

3. Responsibilities

3.1 The Director of Strategic Planning and Governance has overall responsibility for this Complaint Process and has delegated operational responsibility to the University's Data Protection Officer. The Director of Strategic Planning and Governance will be informed of any complaints made under this process and of the outcomes of any complaints investigated under this Process.

3.2 All University staff/employees are responsible for ensuring that any complaints made under this process are reported to the Data Protection Officer/Information Governance Team (information-governance@lancaster.ac.uk) without delay.

3.3 All University staff/employees are responsible for cooperating with the Data Protection Officer (or their nominated deputy) in reviewing and investigating any complaints made under this process.

3.4 Records of all complaints, outcomes of complaint investigations, will be maintained by the Information Governance Team in line with the University's data retention schedules. These records will include: the date the complaint was received, the University's acknowledgement, any relevant conversations, documents and investigation details, the outcome of the complaint, and any actions taken as a result of the complaint investigation.

4. Making a complaint

4.1 All complaints made under this process must be actionable and contain sufficient information to allow their consideration and/or investigation.

4.2 The University will only accept complaints under this process from the individual whose personal data is the subject of the complaint (the 'data subject'), or from their nominated representative.

4.3 Complaints from a data subject's representative, or involvement in the complaint from a data subject's representative, will only be accepted where the representative provides the data subject's written consent authorising the representative to act on the data subject's behalf in relation to the complaint or where the representative provides proof that they are authorised to act on the data subject's behalf, e.g. an appropriate power of attorney or a signed letter of authority from the data subject they are acting on behalf of.

4.4 The University reserves the right to contact the data subject, independent of the representative, to verify such consent or authority. Where no evidence is provided that a representative is authorised to act on behalf of a data subject, the University will not investigate the complaint until appropriate authority is received.

4.5 The University reserves the right to refuse a data subject's choice of representative but will only do so where there is a clear conflict of interest or where it believes the data subject's consent to such a representative is not freely given, unambiguous and explicit (where special category data is likely to be divulged to the representative as part of the Complaint Process).

4.6 If there is doubt about the identity of a complainant, or their representative, the University reserves the right to conduct reasonable and proportionate identity checks. This may involve complainant's, or their representative's, being required to provide proof of identity.

4.7 This Complaints process is not intended to be a legal process. Where a data subject wishes to use a legal representative, it is likely that the complaint process will be delayed whilst the University seeks their own legal advice. Where this is the case, data protection complaints must still be acknowledged within 30 calendar days of receipt.

5. Process

5.1 Upon receipt of a Data Protection Complaint, the Information Governance Team will acknowledge receipt of the complaint without undue delay. Notwithstanding this, all complaints must be acknowledged within 30 calendar days. The 30 calendar days start the day after a complaint is received by the University.

5.2 Communications with complainants will primarily be conducted over email, however, the Information Governance Team will consider requests from complainants to communicate via other means, e.g. verbally, in a written letter, etc.

5.3 Subject to the provisions in 4.1 and 7.1 of this process, complaints will be investigated by the University's Data Protection Officer or nominee without undue delay

5.4 As per 4.1, where a complaint does not contain sufficient information to allow consideration and/or investigation, the Information Governance Team will contact the complainant to ask for further information.

5.5 In the course of the investigation of a complaint, the Data Protection Officer (or nominee) will have free reign to speak to and seek evidence from any member of University staff and/or student.

5.6 The Data Protection Officer (or nominated deputy) will also be entitled to inspect any personal data in relation to the complaint and/or any University systems which holds personal data for which the University is the Data Controller.

5.7 During the investigation of a complaint, the Information Governance Team will keep the complainant updated on the progress of the investigation without undue delay. In practice, this means keeping the complainant up to date with timeframes and explaining any delays, rather than informing them of the steps taken so far.

5.8 Upon completion of the investigation into the complaint, the complaint outcome will be communicated to the complainant in writing, usually by email, without undue delay.

5.9 Complaint outcomes will clearly explain what steps have been taken to resolve the complaint and, where appropriate, any actions taken as a result. Complaint outcomes should provide enough information to help the complainant understand how the outcome has been reached.

5.10 All complaint outcome communications will advise the complainant that they have the right to complain to the Information Commissioner's Office (ICO)/Information Commission and include contact details to allow them to do so.

6. Rejection of complaints

6.1 The University reserves the right to reject complaints made under this process where it is deemed that the complaint is manifestly unfounded, abusive or otherwise vexatious. The following will be considered when determining if a complaint is manifestly unfounded, abusive or otherwise vexatious:

- the data subject makes frequent complaints intended to cause disruption, or
- the complaint makes unsubstantiated accusations of wrongdoing against individuals, or
- the data subject has stated that they intend to cause disruption by making the complaint or in conjunction with other data subject processes (e.g. data subject rights requests), whether in the complaint itself or in other communications, or

- the data subject threatens, or is otherwise abusive to individuals, or
- the data subject continues to repeat complaints which have previously been investigated and the outcomes communicated to them.

This is not an exhaustive list, and all complaints will be considered on a case-by-case basis.

6.2 Where a complaint is deemed to be manifestly unfounded, abusive or otherwise vexatious, the data subject will be informed of this in writing. The data subject will also be advised that they retain the right to complain to the ICO/Information Commission.

7. Use of personal data from complaints

7.1 The University will only use complainant personal data, after an outcome has been achieved, where there is a lawful basis for doing so. The University reserves the right to use complainant personal data for internal reporting and evaluation purposes, learning and training purposes, for discussion with appropriate regulators (e.g. ICO), and for the establishment, exercise or defence of legal claims.

7.2 In relation to these purposes, where possible, personal data will be anonymised or pseudonymised before further use.