

Data Protection Complaints Procedure



Document Title: Data Protection Complaints Procedure	Document Type: Procedure
Document Reference: GC-PRO-018	Version Number: 01
Document Owner: Director of Governance & Compliance	
Equality Impact Assessment Completed By: Director of People and OD	Equality Impact Assessment Date: 11 June 2026
Approved By: Executive Team	Date Approved: 2 June 2026
Issue Date: 12 June 2026	Review Date: 12 June 2028

Version Level	Details of Change	Date
01	This is a new document ensuring compliance with the Data (Use and Access) Act 2025 which requires all organisations to have a Data Protection Complaints Procedure in place by 19 th June 2026.	12/06/2026

Key search words for this document
Data protection, complaints, data protection lead, ICO

Linked Documents
Data Protection Policy Privacy Notice Personal Data Breach Notification Procedure Data Breach Reporting Procedure Subject Access Request Procedure

If you need this information in a different format or language, would like someone to help explain it to you or require any other support please let us know by emailing start@gateshead.ac.uk or calling 0191 490 0300.

This front page is for monitoring and dissemination purposes only.
It does not form part of this Procedure document.

1. Introduction

- 1.1. This procedure applies to all personal data processed by, or on behalf of, Gateshead College, including data relating to students, applicants, employees, governors, contractors, alumni and members of the public.
- 1.2. Gateshead College is committed to delivering a high-quality service. We recognise that, at times, individuals may wish to raise concerns about how their personal data has been handled. We welcome feedback and use complaints as an opportunity to learn, improve and strengthen our practice.

2. Scope

- 2.1. This procedure explains how individuals can raise concerns about how Gateshead College collects, uses, stores or otherwise processes personal data.
- 2.2. It ensures that complaints are handled fairly, transparently and in line with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act.
- 2.3. It also provides a clear internal process for resolving concerns before escalation to the Information Commissioner's Office (ICO), where appropriate.
- 2.4. Individuals have the right to raise a complaint if they believe the College has not complied with data protection legislation or has not handled their personal data appropriately.
- 2.5. Complaints may relate to any aspect of personal data processing, including:
 - The collection or use of personal data
 - The handling of, or response to, data subject rights requests
 - Concerns about the College's Privacy Notice
 - The sharing of personal data with third parties
 - The use of personal data for direct marketing or profiling
 - Failure to comply with the College's data protection policies
- 2.6. All complaints will be considered promptly and transparently and will be investigated by the Data Protection Lead or an appropriate delegated officer.

3. Who Can Make a Complaint

- 3.1. Complaints may be made by:
 - Students or apprentices
 - Prospective students or applicants
 - Parents, carers or guardians
 - Employees or former employees
 - Governors
 - Contractors or suppliers
 - Members of the public
- 3.2. Complaints may also be submitted by an authorised representative acting on behalf of an individual.

4. Principles

- 4.1. The College will ensure individuals are aware of their right to complain, including through its Privacy Notice and communications relating to data rights.
- 4.2. All complaints will be taken seriously and resolved as quickly as possible. Wherever appropriate, the College will seek to resolve concerns informally at an early stage.
- 4.3. Complaints will be managed in a way that is fair, transparent and proportionate, supporting a culture of continuous improvement.
- 4.4. The College will aim to follow this procedure at all times. Where this is not possible (for example during closure periods), any delays will be communicated clearly and promptly.

5. Recording and Monitoring

- 5.1. All complaints are recorded centrally and monitored to identify themes and trends.
- 5.2. This information is used to inform service improvements and enhance the overall experience of students and stakeholders.
- 5.3. Oversight is maintained through regular reporting and review.

6. How to Submit a Complaint

- 6.1. Complaints should, wherever possible, be submitted in writing to:

Data Protection Lead

Gateshead College
Baltic Campus
Quarryfield Road
Baltic Business Quarter
Gateshead
NE8 3BE

Email: DPLead@gateshead.ac.uk

- 6.2. If a complaint is made verbally, the College may ask for this to be confirmed in writing to support proper investigation and record keeping.
- 6.3. The Data Protection Lead will normally acknowledge receipt within 5 working days.
- 6.4. Where appropriate, identity verification may be required before progressing the complaint.
- 6.5. To support a timely investigation, complainants are encouraged to provide:
 - Name and contact details
 - A clear description of the concern
 - Details of the personal data involved (if known)
 - Relevant dates or circumstances
 - Copies of any supporting correspondence

7. Acknowledgement

- 7.1. Upon receipt, the College will acknowledge the complaint within 5 working days.
- 7.2. The acknowledgement will confirm:

- That the complaint has been received
- Who is responsible for investigating it
- The expected timescale for a response

8. Investigation

8.1. The Data Protection Lead will assess the complaint and determine the appropriate course of action. This may include:

- Reviewing relevant policies and procedures
- Examining records and systems
- Liaising with staff involved
- Requesting further information where needed

8.2. Relevant internal teams (such as IT, HR or Student Services) may be consulted where appropriate.

8.3. Investigations will be conducted fairly, impartially and in proportion to the issues raised.

9. Response

9.1. The College will aim to provide a formal written response within one calendar month of receiving the complaint (subject to identity verification where required).

9.2. Where a complaint is complex or requires further clarification, this timeframe may be extended by up to a further two months. Any extension and the reasons for it will be communicated clearly.

9.3. The response will include:

- The outcome of the investigation
- Whether the complaint is upheld or not upheld
- Any actions taken
- Steps taken to prevent recurrence

10. Outcomes

10.1. Where a complaint is upheld, appropriate action will be taken.

10.2. This may include:

- Correcting or updating personal data
- Restricting or stopping certain processing activities
- Improving processes or controls
- Providing additional staff training
- Issuing an apology where appropriate

10.3. Where relevant, the College will consider whether the issue constitutes a personal data breach and whether this should be reported to the ICO.

11. Escalation

- 11.1. If a complainant is not satisfied with the College's response, they may request an internal review within one month of the decision.
- 11.2. Reviews will normally be completed within 20 working days by an appropriate member of the Executive Team or Senior Management Team.
- 11.3. If the complainant remains dissatisfied, they have the right to raise their concern with the Information Commissioner's Office (ICO).
- 11.4. Further information is available at:
<https://ico.org.uk/make-a-complaint/>
- 11.5. The ICO is the UK's independent authority responsible for upholding information rights.

Contact details:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
www.ico.org.uk

- 11.6. The ICO generally expects individuals to have raised concerns with the organisation first before contacting them.

12. Record Keeping

- 12.1. The College maintains a record of all data protection complaints received.
- 12.2. This includes:
 - Date received
 - Nature of the complaint
 - Actions taken
 - Outcome
 - Any corrective measures implemented
- 12.3. This supports the College's accountability obligations under data protection legislation.