DATA PROTECTION COMPLAINTS HANDLING POLICY

1. Purpose

This policy sets out how Durham Students Union handles complaints relating to data protection and the processing of personal data, in line with UK GDPR and ICO guidance.

2. What Is a Data Protection Complaint?

A data protection complaint is any expression of dissatisfaction regarding:

- How we process personal data
- Failure to respond to a data subject rights request
- Alleged misuse, loss or inaccuracy of personal data
- Concerns about transparency, retention or sharing

Complaints may be received via email, phone, webform, post, or verbally. All staff must treat any such expression of concern as a potential data protection complaint.

3. Roles and Responsibilities

All Staff

- Must recognise and promptly report any expression of dissatisfaction relating to personal data.
- Must forward complaints to their line manager and/or the Data Protection Officer without undue delay.
- Must not attempt to dismiss or ignore concerns raised by individuals.

Department Managers / Service Leads

- May handle straightforward data protection complaints within their area of responsibility, where:
    - The issue is clear and low risk (e.g. simple rectification, straightforward erasure request, minor clarification of processing); and
    - They are confident they understand the applicable UK GDPR requirements; and
    - No complex legal interpretation or risk assessment is required.
- Must ensure:
    - The complaint is logged in the Complaints Register.
    - Acknowledgement is issued within 30 days.
    - The response is documented.
- Must escalate the complaint to the Data Protection Officer (DPO) immediately where:
    - The issue involves potential non-compliance or breach.
    - The complaint is complex or high risk.
    - There is uncertainty about the legal basis or appropriate response.
    - The complainant indicates an intention to escalate to the ICO.
    - The matter could result in reputational, financial, or regulatory risk.

4. Complaint Handling Procedure

Step 1 – Logging

- Record in the Complaints Register:
    - Date received
    - Complainant details
    - Nature of complaint
    - Relevant department
    - Assigned handler
    - Deadline dates

Step 2 – Acknowledgement

- Acknowledge receipt within 30 calendar days.
- Confirm next steps and likely timeframe.

Step 3 – Investigation

- Review relevant systems and records.
- Speak to relevant staff.
- Assess compliance with UK GDPR obligations and consult DPO.
- Identify any remedial action required.

Investigations must be conducted without undue delay.

Step 4 – Response

Provide a clear written response explaining:

- What was investigated
- Findings
- Actions taken (if any)
- Any corrective measures
- Right to escalate to the ICO

Step 5 – Record Keeping

Maintain:

- Complaint details
- Investigation notes
- Correspondence
- Outcome
- Actions implemented

Records must be retained for 3 years.

5. Escalation

Where a complainant remains dissatisfied, they must be informed of their right to lodge a complaint with the ICO.

6. Monitoring & Review

- Complaints trends reviewed quarterly.
- Policy reviewed annually.
- Training provided to staff annually.