



DUAA Data Protection Complaints Policy and Procedure

1. Purpose

This policy establishes the process for handling complaints relating to the Society's collection, use, storage, sharing, retention, or other processing of personal information. The policy is designed to ensure compliance with the UK GDPR, Data Protection Act 2018, and the requirements introduced by the Data (Use and Access) Act 2025 (DUAA), which require organisations to maintain a data protection complaints process, acknowledge complaints within 30 days, investigate appropriately, keep complainants informed, and provide outcomes without undue delay.

2. Scope

This policy applies to:

- Members
- Volunteers
- Employees
- Contractors
- Service users
- Visitors
- Any individual whose personal data is processed by the Society.

This policy covers complaints concerning:

- Collection of personal data
- Use of personal data
- Accuracy of personal data
- Data retention
- Information sharing
- Security of personal data
- Direct marketing communications
- Subject Access Requests
- Individual rights under UK GDPR
- Any other matter relating to data protection compliance.

3. Policy Statement

The Society is committed to:

- Treating all data protection complaints seriously and fairly.
- Providing accessible methods for submitting complaints.
- Investigating complaints impartially.
- Taking appropriate remedial action where necessary.
- Learning from complaints to improve data protection practices.
- Resolving complaints as quickly as possible.
- Complying with all statutory requirements relating to complaint handling.



Individuals will not be disadvantaged or treated less favourably because they have made a complaint.

4. Roles and Responsibilities

Data Protection Officer (DPO) – currently the Society Secretary

The DPO is responsible for:

- Receiving and recording complaints.
- Acknowledging complaints.
- Conducting or coordinating investigations.
- Maintaining complaint records.
- Issuing formal responses.
- Identifying learning and improvement opportunities.

Audit & Risk Committee and the Board

The Audit & Risk Committee is responsible for:

- Oversight of complaint trends.
- Monitoring compliance with this policy.
- Ensuring appropriate resources are available.

Staff, Directors and Committee members

- All staff, Directors/Committee members must:
- Forward any data protection complaint immediately to the DPO via gdpr@heartofengland-coop.co.uk.
- Cooperate with investigations.
- Implement any corrective actions required.

5. How to Make a Complaint

Individuals may submit a complaint through any reasonable communication channel including:

- Email
- Letter
- Telephone
- In person.

The Society will provide reasonable assistance to individuals who need help making a complaint, including those with disabilities or communication difficulties. DUAA specifically requires organisations to take steps to facilitate complaints, for example through electronic means. Complaints should include, where possible:

- Name and contact details
- Description of the concern
- Relevant dates
- Any supporting evidence
- The outcome sought.

6. Complaint Handling Procedure

Stage 1 – Receipt



Upon receiving a complaint:

- a. The complaint will be logged in the Data Protection Complaints Register.
- b. A unique reference number will be assigned.
- c. The date of receipt will be recorded.

Stage 2 – Acknowledgement

The Society will acknowledge receipt of the complaint *within 30 calendar days of receiving it*. The acknowledgement will:

- a. Confirm receipt.
- b. Provide a complaint reference number.
- c. Explain the next steps.
- d. Provide contact details for further communication.

Stage 3 – Assessment

The D PO will determine:

- a. Whether the matter is a data protection complaint.
- b. Whether additional information is required.
- c. Whether urgent risk mitigation is needed.
- d. Whether any potentially reportable data breach exists.
- e. Where necessary, further enquiries will be made with relevant individuals.

The Society will take appropriate steps to investigate complaints and make suitable enquiries as required by the Information Commissioner's Office (ICO) guidance.

Stage 4 – Investigation

The investigation may include:

- a. Reviewing relevant records.
- b. Interviewing relevant personnel.
- c. Examining processing activities.
- d. Reviewing policies and procedures.
- e. Assessing compliance with legal obligations.

The complainant will be kept informed of progress where appropriate. ICO guidance requires organisations to keep complainants informed during the process.

Stage 5 – Outcome

Once the investigation is completed, the complainant will be informed of the outcome without undue delay. The response will include:

- a. A summary of the complaint.
- b. Findings from the investigation.
- c. Any corrective actions taken.
- d. Details of any rights available to the complainant.
- e. Information about escalation to the ICO if the complainant remains dissatisfied.

Possible outcomes include:

- Complaint upheld.



- Complaint partially upheld.
- Complaint not upheld.
- Complaint resolved through agreed action.

7. Escalation to the ICO

If an individual remains dissatisfied after receiving the Society's final response, they may complain to the Information Commissioner's Office (ICO) using [Make a complaint about how an organisation has used your personal information | ICO](#).

The Society encourages individuals to allow it an opportunity to investigate and resolve the matter before approaching the ICO.

8. Complaint Records

The Society will maintain a Data Protection Complaints Register containing:

- Reference number
- Date received
- Complainant name
- Nature of complaint
- Investigation actions
- Outcome
- Closure date
- Lessons learned

Records will be retained in accordance with the Society's retention schedule and kept confidential.

9. Learning and Continuous Improvement

Data protection complaints will be reviewed periodically to identify:

- Recurring issues
- Training needs
- Policy improvements
- Security enhancements
- Governance improvements

Appropriate corrective and preventative actions will be implemented where necessary.

10. Vexatious or Abusive Complaints

The Society will consider all genuine complaints fairly. Where a complaint is clearly abusive, threatening, repetitive without new evidence, or intended solely to harass, the Society may limit communications while still ensuring compliance with its legal obligations. Any such decision must be approved by the DPO and documented.

11. Monitoring and Review

This policy will be reviewed annually; or following significant legislative, regulatory, or organisational changes. The policy will be updated to reflect changes in UK data protection law, ICO guidance, and DUAA requirements.