Data Protection Complaints Handling Process

1. Purpose

The purpose of this Data Protection Complaints Handling Process ("Process") is to provide a fair, transparent, and effective mechanism for individuals to raise concerns regarding the processing of their personal data and to ensure compliance with:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018 (DPA 2018);
- Data (Use and Access) Act 2025 (DUAA);
- Information Commissioner's Office (ICO) guidance on data protection complaints

This Process applies to all complaints received on or after 19 June 2026.

2. Scope

This Process applies to complaints relating to:

- Collection of personal data;
- Use of personal data;
- Disclosure or sharing of personal data;
- Data retention practices;
- Data security measures;
- Direct marketing activities;
- Automated decision-making;
- International transfers of personal data;
- Handling of data subject rights requests;
- Personal data breaches;
- Any alleged infringement of UK data protection legislation.

This Process applies to complaints from:

- Customers;
- Employees;
- Job applicants;
- Contractors;
- Suppliers;
- Website users;
- Any individual whose personal data is processed by the Organisation.

3. Definitions

Data Protection Complaint

A complaint made by or on behalf of an individual alleging that the Organisation has failed to comply with UK data protection legislation in relation to personal data.

A complaint does not need to:

- Refer to legislation;
- Use legal terminology;
- Be labelled as a "data protection complaint."

Any expression of dissatisfaction relating to the handling of personal data must be considered for assessment under this Process.

Complainant

The individual making the complaint or their authorised representative.

4. Complaints Principles

The Organisation will ensure that all data protection complaints are:

- Handled fairly and impartially;
- Investigated objectively;
- Managed without undue delay;
- Documented appropriately;
- Resolved at the earliest opportunity;
- Escalated where necessary;

Used as a source of organisational learning.

5. Making a Complaint

The Organisation shall facilitate the making of data protection complaints through multiple accessible channels.

Complaints may be submitted via:

- Email;
- Online complaint form;
- Website contact form;
- Post;
- Telephone;
- In person;
- Live chat services;
- Social media channels;
- Any employee of the Organisation.

Individuals shall not be required to use a specific complaint channel.

Where a complaint is received by an employee, the employee must immediately forward the complaint to the Data Protection Team.

6. Information Provided to Individuals

The Organisation shall inform individuals:

- Of their right to complain to the Organisation;
- How complaints can be submitted;
- Of their right to complain to the Information Commissioner's Office (ICO);
- How the complaint will be handled.

This information shall be included within:

- Privacy Notices;
- Data Subject Rights correspondence;
- Complaint acknowledgement letters;
- The Organisation's website.

7. Complaint Receipt and Logging

Upon receipt of a complaint, the Organisation shall:

1. Create a complaint record.
2. Assign a unique reference number.
3. Record:
   - Date received;
   - Complainant details;
   - Nature of complaint;
   - Relevant processing activities;
   - Assigned investigator;
   - Deadlines and actions.

All complaints shall be entered into the Data Protection Complaints Register.

8. Acknowledgement

The Organisation shall acknowledge receipt of the complaint within thirty (30) calendar days of receipt.

The acknowledgement shall include:

- Complaint reference number;
- Name or role of investigator;
- Summary of the complaint;
- Expected next steps;
- Contact details for further enquiries;

Information regarding the complainant's rights.

9. Initial Assessment

Within ten (10) working days of allocation, the investigator shall determine:

- Whether the matter constitutes a data protection complaint;
- Whether additional information is required;
- Whether immediate remedial action is necessary;
- Whether the complaint indicates a personal data breach;
- Whether escalation is required.

Where clarification is needed, the investigator shall contact the complainant promptly.

10. Investigation

The investigator shall conduct an appropriate and proportionate investigation.

Activities may include:

- Reviewing relevant records;
- Interviewing personnel;
- Examining technical logs;
- Reviewing policies and procedures;
- Assessing legal obligations;
- Consulting the Data Protection Officer (DPO);
- Consulting Legal Counsel where required.

The Organisation shall make appropriate enquiries and keep the complainant informed of progress where investigations are ongoing.

11. Escalation Criteria

The complaint shall be escalated to the Data Protection Officer immediately if:

- Special category data is involved;
- Criminal offence data is involved;
- A personal data breach is suspected;
- Significant regulatory risk exists;
- Multiple individuals are affected;
- Legal proceedings are threatened;
- The complaint raises systemic compliance concerns.

12. Complaint Outcomes

Following investigation, the Organisation may determine that:

Complaint Upheld

The Organisation accepts that a breach of data protection requirements has occurred.

Actions may include:

- Apology;
- Corrective action;
- Rectification of personal data;
- Erasure of personal data;
- Restriction of processing;
- Additional staff training;
- Process improvements.

Complaint Partially Upheld

The Organisation accepts some aspects of the complaint but not all.

Complaint Not Upheld

The Organisation concludes that data protection obligations were met.

13. Response to the Complainant

The Organisation shall provide the outcome of the complaint without undue delay.

The final response shall include:

- Summary of the complaint;
- Investigation undertaken;
- Findings;
- Actions taken or proposed;
- Explanation of decisions made;
- Information regarding escalation rights.

The response shall also explain the individual's right to complain to the Information Commissioner's Office if dissatisfied.

14. ICO Escalation Information

The Organisation shall inform complainants that they may contact:

Information Commissioner's Office (ICO)
Website: https://www.ico.org.uk

The Organisation shall cooperate fully with any subsequent ICO investigation.

15. Personal Data Breach Identification

Where a complaint reveals a potential personal data breach, the matter shall immediately be referred to the Organisation's Personal Data Breach Response Procedure.

The complaint investigation and breach investigation may proceed in parallel.

16. Record Keeping

The Organisation shall maintain records of:

- Complaints received;
- Acknowledgements issued;
- Investigation activities;
- Communications with complainants;
- Outcomes;
- Corrective actions;
- Lessons learned.

Records shall be retained in accordance with the Organisation's Retention Schedule.

17. Monitoring and Reporting

The Data Protection Officer shall review complaint data at least quarterly.

Reports shall include:

- Number of complaints received;
- Categories of complaints;
- Response times;
- Outcomes;
- Root causes;
- Trends and recurring issues;
- Corrective actions implemented.

Management shall review reports to identify opportunities for improvement.

18. Training

All employees shall receive training covering:

- Recognition of data protection complaints;
- Escalation procedures;
- Complaint handling obligations;
- UK GDPR requirements;
- ICO expectations.

Training shall be refreshed at least annually.

19. Continuous Improvement

The Organisation shall periodically review:

- Complaint trends;
- Root causes;
- Policy effectiveness;
- Regulatory developments;
- ICO guidance.

Processes shall be updated where necessary to maintain compliance and improve customer outcomes.

20. Review

This Process shall be reviewed:

- Annually;
- Following significant complaints;
- Following regulatory changes;

Following ICO enforcement action or guidance updates.

21. Document Control

Document Owner: Data Protection Officer
Approved By: Senior Management
Review Frequency: Annual
Effective Date: 19th June 2026
Version: 1.0