to be your best

Data Protection Complaints Policy.

TRUE.Values.

Purpose

This policy outlines how OCS Group Holdings Ltd and its subsidiaries ("OCS") handle complaints relating to the processing of personal data, in accordance with the Data Protection Act 2018 (as amended by the DUAA 2025), UK GDPR, and other applicable legislation.

Scope

This policy applies to all OCS employees, contractors, and third-party processors. It covers complaints made by individuals (data subjects) regarding how their personal data is collected, used, stored, shared, or otherwise processed by OCS.

Definition of a Data Protection Complaint

A data protection complaint is any expression of dissatisfaction from a data subject regarding:

- A data breach affecting their personal data
- The handling of a Data Subject Access Request (DSAR)
- The retention period of their data
- Automated decision-making or profiling
- Any other matter relating to the processing of their personal data

How to Make a Complaint

Individuals may submit complaints in the following ways:

- Using the online form: Data Protection Complaints Form
- Or via email: dataprotection@ocs.com

Staff Responsibilities

All staff should:

- Recognise and report data protection complaints promptly
- Direct complaints to the Data Protection Team at dataprotection@ocs.com
- Assist with investigations when required

Complaints Handling Procedure

OCS will follow a five-step process:

Step 1: Acknowledge

Complaints will be acknowledged within 2 working days of receipt. Acknowledgement may be via email, post, or phone depending on the method of submission.

Step 2: Investigate

Investigations will be conducted without undue delay. The Data Protection Officer will gather relevant facts, consult internal stakeholders, and assess compliance with internal policies and legal obligations.

Step 3: Update

Complainants will be kept informed of progress. If delays occur, OCS will provide an estimated resolution date and a point of contact.

Step 4: Outcome

A written response will be provided as soon as possible. The response will include:

- Findings of the investigation
- Any remedial actions taken
- Information on the right to escalate to the ICO

Step 5: Record Keeping

OCS will maintain records of:

- Complaint received date
- Acknowledgement
- Investigation notes
- Outcome and actions taken
- Any escalation to the ICO

Complaint Escalation

Escalation to Senior Management

The complainant may request that the matter be escalated to the Group Data Protection Officer (DPO) or a designated member of the Executive Leadership Team. The escalation request must include:

- A summary of the original complaint
- The outcome of the internal review
- Reasons for escalation

A senior-level review will be conducted within 15 working days, and a final written response will be issued.

Escalation to External Authorities

If the complainant is still not satisfied after internal escalation, they may escalate the matter to the Information Commissioner's Office (ICO) or other relevant supervisory authority.

OCS will cooperate fully with any external investigation and provide all necessary documentation and records.

Legal Recourse

Complainants may also seek legal advice or pursue remedies through the courts if they believe their rights under data protection law have been infringed.

Monitoring and Review

This policy will be reviewed annually or upon significant legislative change.

Document Control

Version	Description	
1.0 New policy following implementation of Data Use and Access Act 2025	**Date live**	**September 2025**
	Author	**Sara Taylor, DPO**
	Approved by	