FLX Health Ltd
31-38 Queen Street
Hull, Humberside HU1 1UU
United Kingdom

Company Name: FLX Health LTD

Effective Date: 03/06/2025

Policy Owner: Directors

1. Purpose & Scope

This policy outlines how FLX Health Ltd handles complaints regarding the collection, storage, use, or protection of personal data. It applies to all external individuals (customers, suppliers, partners) and internal employees who wish to raise a data protection concern.

2. How Complaints are Received (Intake Method)

We are committed to making it simple for individuals to voice concerns. Complaints can be submitted through the following official channels:

- **Email:** help@flx.health

Note to Team: Any employee who receives a data protection complaint via phone or general email must forward it to the Policy Owner within **24 hours**.

3. Review & Investigation Process

Upon receipt, the complaint will undergo a structured, independent review handled by the Policy Owner:

- **Log & Acknowledge:** The complaint is logged in our internal Data Protection Register and assigned a unique reference number.

- **Initial Assessment:** The Policy Owner assesses the severity of the alleged breach (e.g., individual error, systemic system flaw, or potential reportable data breach).

- **Investigation:** The Policy Owner will interview relevant staff, review access logs, and audit data handling processes to determine if a policy violation occurred.

- **Corrective Action:** If a gap is identified, an immediate remediation plan will be enacted (e.g., software patches, staff retraining, process updates).

4. Response Timeframes

In line with UK regulatory best practices and to avoid internal confusion, we adhere to the following strict timelines:

- **Acknowledgement:** Sent to the complainant within **3 working days** of receipt.

- **Full Resolution & Response:** A formal, written response detailing our findings and actions taken will be issued within **30 calendar days**.

- **Extensions:** If a case is highly complex, we may extend the timeline by an additional 30 days, but we must notify the complainant of the delay and the reason within the initial 30-day window.

5. Record Keeping & Auditing

To maintain compliance and prepare for potential regulatory audits, the company maintains a centralised **Data Protection Complaints Log**. This log details:

- Date received and unique case ID.

- Nature of the complaint (e.g., marketing opt-out failure, subject access request delay).

- Investigation findings and internal root-cause analysis.

- Final outcome, response sent date, and preventative actions taken.

All records under this policy are kept securely for a minimum of **6 years** from the date of resolution.

6. Escalation to the Regulator

If the complainant remains unsatisfied with our final response, they retain the right to escalate the matter to the UK supervisory authority:

- **Authority:** Information Commissioner's Office (ICO)
- **Website:** www.ico.org.uk

Review and Evaluation:

This Data Protection Complaints policy will be reviewed annually to ensure its effectiveness and relevance to our business operations. Any necessary adjustments will be made to further enhance our environmental performance.

This policy was last reviewed in May 2026