Data Protection and GDPR Complaints Handling Procedure

Document Owner: Director of People Operations, DPO		
Version No.	**Date**	**Notes**
1	June 2026	Creation of policy (Samantha Hackett)

Purpose and Scope

Cambridge Spark is fully committed to compliance with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We respect the privacy rights of all individuals whose personal data we collect, store, and process.

The purpose of this procedure is to outline a clear, structured, and legally compliant framework for handling complaints relating to data protection, privacy, and the exercise of individual data subject rights.

Unlike general or delivery complaints, this procedure is global in scope. It applies to any individual whose personal data is processed by Cambridge Spark, including but not limited to:

- Current, prospective, and former learners
- Corporate clients and community stakeholders
- Full-time, part-time, and casual employees
- Freelancers and independent contractors
- Job applicants and prospective candidates
- Website visitors and external suppliers

Definitions of Common Complaint Types

For the purpose of this document, a data protection complaint is defined as any expression of dissatisfaction concerning how Cambridge Spark collects, stores, uses, shares, or retains personal data.

Common types of complaints handled under this procedure include:

- **Rights Fulfillment Disputes:** Claims that Cambridge Spark has failed to properly fulfill a Subject Access Request (SAR), a request for data erasure ("right to be forgotten"), data rectification, restriction of processing, or data portability.
- **Unauthorised Disclosure/Breaches:** Concerns that personal information has been shared with unauthorised third parties or exposed through a security incident.
- **Inaccurate Records:** Dissatisfaction regarding the accuracy of personal records held by the company and an alleged failure to update or correct them.
- **Non-Compliance with Principles:** Allegations that data has been processed unlawfully, unfairly, without transparency, or kept longer than necessary.

Key Roles and Responsibilities

Data Protection Officer (DPO): The DPO holds overarching responsibility for investigating data protection complaints, assessing legal risks, and ensuring corporate compliance with regulatory timelines. The DPO acts as the primary point of contact for data subjects and regulatory authorities.

Complaints & Intake Teams: Any staff member monitoring general company communication lines is responsible for instantly identifying and routing any data privacy issues directly to the DPO.

All Staff: All employees must cooperate fully and promptly with the DPO during data handling investigations, ensuring that internal records, software logs, and communications are provided immediately upon request.

Procedure for Raising a Complaint

All data protection and GDPR-related complaints must be submitted in writing to the dedicated privacy mailbox: **privacy@cambridgespark.com**.

Complainants should provide a clear outline of their concern, including what personal data is involved, any relevant dates, names of staff members contacted, and their desired resolution.

If a data privacy complaint is accidentally sent to the general complaints mailbox, the quality and admin teams will execute an immediate internal transfer to the privacy inbox within 24 hours.

Identity Verification Protocol

To prevent the unauthorised exposure of personal data, Cambridge Spark must securely verify the identity of the complainant before disclosing any internal investigation details, logs, or system data.

The DPO may request proportional evidence of identity, such as a confirmed email address match, internal account identifiers, or photographic identification if necessary.

If a complaint is submitted by a third party (such as a legal representative, parent, or guardian) on behalf of a data subject, it will only be processed upon receipt of an explicit, signed Third-Party Data Release Authorisation form from the affected individual.

Strict Investigation and Response Timelines

Data protection legislation enforces strict statutory time limits. All GDPR complaints must follow these precise milestones:

Stage	**Action Required**	**Statutory Window**
1. Acknowledgement	DPO logs the complaint and issues a formal written receipt to the sender	Within 48 hours of receipt

2. Review & Assessment	DPO determines if a data breach has occurred and coordinates with IT/Systems	Within 7 working days
3. Full Resolution Response	DPO issues the definitive outcome, corrective actions and escalation rights	Maximum of 1 calendar month

Complex Cases: If an investigation is highly complex, the DPO may extend the response window by up to an additional two months. In such cases, the complainant must be formally notified in writing before the initial one-month deadline expires, detailing the specific technical reasons for the delay.

Escalation to the Information Commissioners Office (ICO)

If a complainant is dissatisfied with the DPO's final investigation outcome or the manner in which their data protection complaint was handled, they maintain the legal right to lodge a complaint directly with the national data protection supervisory authority.

The regulatory authority for Cambridge Spark is the UK Information Commissioner's Office (ICO). The DPO will include the ICO's standard contact channels in all final resolution letters:

- Postal Address: Information Commissioner's Office, Wycliffe House, Water Lane,
- Wilmslow, Cheshire, SK9 5AF
- Helpline Number: 0303 123 1113
- Official Website: www.ico.org.uk

Confidentiality, Logging and Audit Retention

All records concerning data protection complaints, including the original intake emails, investigation logs, system evidence, and outcome letters, are strictly confidential.

These records are maintained by the DPO in a secure, encrypted internal compliance folder, separate from standard learner or human resources databases.

In strict alignment with legal guidelines, all documentation within the data protection complaints log will be securely retained for a fixed audit period of six (6) years from the date of final resolution, after which it will be permanently deleted.

Senior Manager Sign-off

Name: Tom Phillips

Position: COO

Signed: 

Date: 19 June 2026