



# Consalia Limited

## Data Protection Policy

### Revision History

V1.0		Issued
v1.1		Review and minor amendments
v1.2	31/1/2019	Review and minor amendments
v1.3	20/2/2021	Updated with new Consalia branding
V1.4	9/11/2021	Review with minor amendments
V1.5	17/1/2024	Update of Cyber Essentials Plus details
V2	29/10/2024	Redraft of Policy

## Table of Contents

<b>1. INTRODUCTION</b>	<b>4</b>
<b>2. PURPOSE AND SCOPE</b>	<b>4</b>
<b>3. KEY PRINCIPLES OF DATA PROTECTION</b>	<b>4</b>
<b>4. ROLES AND RESPONSIBILITIES</b>	<b>5</b>
<b>5. DATA COLLECTION AND PROCESSING</b>	<b>5</b>
<b>6. DATA SUBJECT RIGHTS</b>	<b>5</b>
<b>7. DATA SECURITY MEASURES</b>	<b>6</b>
<b>8. DATA SHARING AND THIRD-PARTY PROCESSING</b>	<b>6</b>
<b>9. DATA RETENTION AND DISPOSAL</b>	<b>6</b>
<b>10. DATA BREACH PROCEDURES</b>	<b>6</b>
<b>11. TRAINING, AWARENESS, AND ACCESSIBILITY</b>	<b>7</b>
<b>12. ACCOUNTABILITY AND GOVERNANCE</b>	<b>7</b>
<b>13. POLICY REVIEW AND AMENDMENTS</b>	<b>7</b>
<b>APPROVAL AND ACKNOWLEDGEMENT</b>	<b>7</b>

# Data Protection Policy for Consalia Ltd

## 1. Introduction

Consalia needs to keep certain information about its employees, students, apprentices and other users to allow us to monitor recruitment, attendance, performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. Consalia Ltd. is committed to upholding the highest standards of data protection, ensuring the confidentiality, integrity, and availability of all personal data under our control. This policy sets out Consalia's approach to managing personal data responsibly, in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. It applies to all employees, contractors, and any third parties involved in data processing on behalf of Consalia. Compliance with this policy is mandatory, and failure to adhere may result in disciplinary action. Consalia will keep a register of staff authorised to access and process learner and staff data and these members of staff will be asked to sign a confidentiality agreement.

## 2. Purpose and Scope

This policy aims to:

- Protect the privacy and rights of individuals whose data we collect, process, and store.
- Ensure that personal data is managed in a lawful, transparent, and secure manner.
- Establish a clear framework of responsibilities and procedures to maintain data integrity and security.

The policy covers all types of personal data processed by Consalia, including but not limited to, employee records, client information, and data associated with students or training participants. It applies to all data collected in any form—whether digital, paper-based, or other storage media—and all individuals who have access to or process this data.

## 3. Key Principles of Data Protection

Consalia Ltd. upholds the following data protection principles as set forth in the GDPR:

1. **Lawfulness, Fairness, and Transparency:** Data is collected and processed lawfully, with fairness to individuals, and in a transparent manner.
2. **Purpose Limitation:** Data is collected for specified, explicit, and legitimate purposes, and will not be further processed in ways that are incompatible with those purposes.
3. **Data Minimisation:** Only the minimum necessary data is collected and retained to meet business and legal requirements.
4. **Accuracy:** Consalia is committed to maintaining accurate and up-to-date data, making corrections promptly upon request.
5. **Storage Limitation:** Data will be retained for only as long as necessary, based on defined retention schedules, after which it will be securely disposed of.

6. **Integrity and Confidentiality (Security):** Appropriate security measures are taken to ensure data protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
7. **Accountability:** Consalia takes full responsibility for complying with data protection principles and will demonstrate this compliance upon request.

## 4. Roles and Responsibilities

- **Data Controller:** Consalia Ltd. determines the purposes and means of processing personal data and ensures compliance with data protection obligations.
- **Data Protection Officer (DPO):** The DPO is responsible for overseeing data protection strategy and implementation, handling data subject requests, conducting regular audits, and liaising with the Information Commissioner's Office (ICO) as necessary. The DPO is also the point of contact for data protection issues and can be reached at [psquire@consalia.com](mailto:psquire@consalia.com)
- **Employees and Contractors:** All employees and contractors must familiarise themselves with this policy and handle personal data in compliance with it. Employees are required to report any suspected data breaches or non-compliance incidents to the DPO immediately.

## 5. Data Collection and Processing

Consalia will collect and process personal data only for legitimate business and operational purposes, or where there is a legal obligation. When collecting data, individuals will be informed of the purpose, the legal basis for processing, and how the data will be used.

Data processing will only extend to what is necessary, in compliance with GDPR requirements, and data will be kept accurate and up-to-date. Any sensitive data, such as health or demographic information, will require explicit consent from the data subject or be processed according to legal obligations.

## 6. Data Subject Rights

Under the GDPR, data subjects have rights in relation to their personal data. Consalia respects and upholds these rights:

1. **Right to Access:** Individuals can request to view the personal data Consalia holds about them.
2. **Right to Rectification:** Individuals can request that inaccurate data be corrected.
3. **Right to Erasure:** In certain circumstances, individuals may request the deletion of their data (also known as the 'right to be forgotten').
4. **Right to Restrict Processing:** Individuals can request that the processing of their data be restricted if they contest its accuracy or if the processing is unlawful.
5. **Right to Data Portability:** Consalia will, where feasible, provide personal data in a structured, commonly used, and machine-readable format upon request.

6. **Right to Object:** Individuals have the right to object to data processing, including processing for direct marketing purposes.
7. **Rights in Relation to Automated Decision-Making:** Individuals have the right not to be subject to decisions made solely by automated means if these significantly affect them.

## 7. Data Security Measures

Consalia is committed to maintaining robust data security measures to prevent unauthorised access, alteration, or destruction of personal data. Key security practices include:

- **Technical Controls:** Consalia uses industry-standard firewalls, encryption, and secure access controls. All personal data is stored in secured databases and protected by multi-factor authentication.
- **Physical Security:** Personal data in physical form (e.g., paper records) is stored in locked cabinets accessible only to authorised personnel.
- **Incident Reporting:** Employees are trained to recognise and report any suspected data breaches or near-miss incidents immediately to the DPO.
- **Regular Training:** All employees receive regular training on data protection and security practices. Periodic assessments are conducted to verify understanding and compliance.

## 8. Data Sharing and Third-Party Processing

Personal data may be shared with third parties only when it is essential to fulfil a legitimate business purpose, or where legally required. When engaging third-party processors, Consalia will:

- Conduct due diligence to ensure that the third party can meet the necessary data protection standards.
- Enter into legally binding data processing agreements with all third-party data processors.
- Ensure that personal data will not be transferred outside of the European Economic Area (EEA) unless the destination country provides adequate data protection standards, or specific safeguards are in place.

## 9. Data Retention and Disposal

Personal data will be retained only for as long as is necessary for the purposes for which it was collected or as required by law. Consalia has implemented retention schedules to manage the lifecycle of data, with regular audits to assess compliance. Data will be securely disposed of after the retention period, whether by shredding, deletion, or de-identification.

## 10. Data Breach Procedures

In the event of a data breach, Consalia has established a protocol to address and report incidents swiftly and in compliance with regulatory requirements:

- **Identification and Containment:** Staff are required to immediately report any potential data breaches to the DPO. The DPO will assess and contain the breach if confirmed.

- **Investigation and Risk Assessment:** The DPO will evaluate the nature and scope of the breach, assess its impact, and determine necessary actions to mitigate risks to data subjects.
- **Notification:** Consalia will notify the ICO of a data breach within 72 hours if it is likely to result in a risk to the rights and freedoms of data subjects. If the breach poses a high risk, affected data subjects will also be informed without undue delay.
- **Record Keeping:** All data breaches, including near misses, are documented in a breach register maintained by the DPO, detailing the nature, impact, and corrective actions taken.

## 11. Training, Awareness, and Accessibility

Consalia is committed to building a culture of data protection awareness through the following measures:

- **Onboarding and Induction:** All new employees are introduced to this policy as part of their onboarding. It will be covered in the induction process for learners and included in their handbooks.
- **Accessibility:** Internal stakeholders can access this policy on the shared drive, while external stakeholders can view it on Consalia's website.
- **Mandatory Training:** All staff must complete data protection training at induction, with refresher sessions provided annually or sooner if significant changes to the policy occur.
- **Policy Review:** The policy will be reviewed annually to ensure it remains up-to-date and responsive to changes in legislation, organisational practices, and technology.

## 12. Accountability and Governance

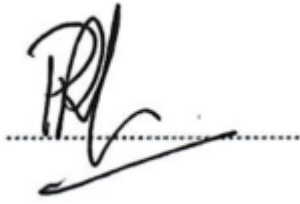
Consalia Ltd. recognises the importance of ongoing accountability in data protection. The DPO is responsible for monitoring policy compliance and conducting regular audits to assess and document compliance with GDPR. The DPO also provides guidance on data protection impact assessments (DPIAs) where high-risk processing activities are identified.

## 13. Policy Review and Amendments

This policy is subject to an annual review by the DPO or sooner if there are material changes in data protection legislation or organisational practices. All amendments will be documented in a revision history, and staff will be informed of any changes. A copy of the current policy will be available on the shared drive for all internal stakeholders.

## Approval and Acknowledgement

This policy was reviewed and approved by

A handwritten signature in black ink, appearing to be 'PS', is written over a horizontal dotted line. A solid horizontal line extends from the end of the dotted line to the right.

Philip Squire on behalf of Consalia Ltd. Senior Management/Board on 29 October 2024.  
Employees are required to acknowledge receipt and understanding of this policy,  
confirming their commitment to uphold the highest standards of data protection at  
Consalia.