Data Protection and Data Security Policy

Statement and Purpose of Policy

StudyBox (the Employer) is committed to ensuring that all personal data handled by us will be processed according to the legally compliant standards of data protection and data security under the UK data protection regime.

For the purposes of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, StudyBox is a data controller of the personal data in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal data is processed.

The purpose of this policy is to help us achieve our data protection and data security aims by:

- Notifying our staff of the types of personal information that we may hold about them, our customers, suppliers, and other third parties and what we do with that information.

- Setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer, and store personal data.

- Ensuring staff understand our rules and legal standards, and clarifying the responsibilities and duties of staff in respect of data protection and security.

This policy does not form part of your contract of employment and may be amended at any time, at our discretion.

Definitions

Criminal records data: information about an individual's criminal convictions and offences, including criminal allegations and proceedings.

Data protection laws: all applicable laws relating to the processing of personal data, including the UK GDPR and Data Protection Act 2018.

Data subject: the individual to whom the personal data relates.

Personal data: any information relating to an identified or identifiable living individual.

Processing: any operation performed on personal data, including collection, storage, alteration, disclosure, or destruction.

Special categories of personal data: information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and biometric data.

Data Protection Principles

Staff must comply with the following principles. Personal information must be:

- Processed lawfully, fairly, and transparently.

- Collected only for specified, explicit, and legitimate purposes.

- Adequate, relevant, and limited to what is necessary.

- Accurate and kept up to date.

- Kept no longer than necessary.

- Processed securely using appropriate technical and organisational measures.

Responsibility for Data Protection and Security

The Senior Responsible Individual (SRI) – previously the Data Protection Officer (DPO) – oversees compliance with this policy. All staff are responsible for compliance, handling personal data consistently with the principles set out here, and protecting data security.

Breaches of this policy will be taken seriously and may result in disciplinary action, up to and including dismissal.

International Data Transfers

Personal data will only be transferred outside the UK where adequate safeguards are in place, in accordance with the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses.

Retention and Storage

Personal data will be retained only as long as necessary for the purposes for which it was collected and will be reviewed annually. Data will be deleted or anonymised when no longer needed.

Individual Rights

Data subjects have the following rights under the UK GDPR:

- Right to access (subject access requests)

- Right to rectification

- Right to erasure (right to be forgotten)

- Right to restriction of processing

- Right to data portability

- Right to object to processing

- Rights related to automated decision-making

Requests will be responded to within **one calendar month** of receipt. Proof of identification may be required.

Data Security Measures

We use technical and organisational measures to keep personal data secure, including:

- Multi-factor authentication (MFA) for access to sensitive systems.

- Encryption and pseudonymisation where appropriate.

- Regular data backups and security software updates.

- Secure physical storage (locked desks/cabinets, restricted server access).

- Mandatory cloud service approval by the SRI.

- Staff training on data handling and cybersecurity.

Personal data must not be stored on unencrypted mobile devices or personal drives.

AI and Automated Decision-Making

StudyBox will assess and document any risks arising from the use of AI or automated decision-making that impacts staff, students, or other data subjects, in compliance with the UK GDPR and ICO guidance.

Data Breaches

All personal data breaches will be logged and assessed. Where a breach poses a risk to individuals' rights or freedoms, it will be reported to the Information Commissioner's Office (ICO) within 72 hours. Where a breach is high risk, affected individuals will be notified.

Training and Review

All staff will receive data protection training at induction and refresher training at least annually. This policy will be reviewed **annually** or sooner if there are significant changes to UK data protection law, including implementation of the Data Protection and Digital Information Act.

Contact

For queries or to exercise your rights under this policy, contact the Senior Responsible Individual at:
shannon@stuydbox.london

This 2025 edition replaces all previous versions of the StudyBox Data Protection and Data Security Policy and incorporates updates from the UK GDPR, Data Protection Act 2018, and anticipated provisions under the Data Protection and Digital Information Bill.