Data Protection, Storage and Retention Policy

1. Policy Statement and Legal Framework

JC Training & Consultancy is fully committed to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all associated privacy and confidentiality legislation. The organisation recognises its responsibility to ensure that personal data is processed lawfully, fairly, and transparently, and that individuals' rights are fully respected at all times.

Personal data is only collected and processed where there is a clear, defined, and legitimate purpose. The organisation ensures that data is adequate, relevant, and limited to what is necessary for operational and statutory requirements. Appropriate technical and organisational measures are in place to protect data from loss, misuse, or unauthorised access, and data is retained only for as long as is necessary in line with legal, regulatory, and funding obligations.

This policy applies to all staff, learners, subcontractors (where applicable), and any third parties processing data on behalf of the organisation.

2. Data Controller and Accountability

JC Training & Consultancy acts as the Data Controller for all personal data processed in the course of its operations. Overall accountability for compliance with UK GDPR rests with the Managing Director, who acts as the designated senior responsible person for data protection.

The Managing Director ensures that appropriate governance arrangements are in place, including oversight of data protection compliance, approval of Data Protection Impact Assessments, and responsibility for breach management and regulatory reporting where required. The organisation ensures that all staff understand their responsibilities in relation to data protection and confidentiality through induction and ongoing training.

3. Purpose and Lawful Basis for Processing

Personal data is processed solely for defined and legitimate purposes connected to the delivery of training and education services. This includes learner enrolment, programme delivery, assessment, certification, and compliance with funding and regulatory requirements. Data is also used to support quality assurance processes, monitor performance, and ensure equality, diversity, and inclusion requirements are met.

The lawful basis for processing is determined in accordance with UK GDPR. In most cases, processing is necessary for the performance of a contract with the learner or employer, or to comply with a legal obligation. In some circumstances, processing is carried out under legitimate interests where this does not override individual rights. Where special category data is processed, such as ethnicity or disability information, this is carried out only where strictly necessary and supported by additional safeguards and, where required, explicit consent.

4. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is undertaken whenever processing is likely to present a high risk to individuals' rights and freedoms. This includes the introduction of new systems, changes to data processing activities, or the use of sensitive personal data at scale.

The purpose of the DPIA process is to identify privacy risks, assess the necessity and proportionality of processing, and implement measures to reduce identified risks. DPIAs are embedded within project planning and system development processes to ensure that data protection is considered from the outset. They are reviewed when significant changes occur to systems, processes, or data usage.

5. Categories of Personal Data Processed

The organisation processes a range of personal data necessary for the delivery of services. This includes core identification data such as names, dates of birth, contact details, Unique Learner Numbers, and National Insurance numbers. It may also include employment information where relevant to programme delivery.

In addition, the organisation processes equality and diversity information, including ethnicity, gender, and disability-related data where disclosed. This information is classified as special category data under UK GDPR and is subject to enhanced protection and stricter access controls.

6. Data Collection, Use, and Information Flows

Personal data is collected at the point of learner engagement, typically during enquiry, enrolment, induction, and initial assessment. The data is recorded in secure internal systems designed for quality assurance and learner management purposes.

Access to personal data is strictly controlled and limited to authorised personnel based on their job role. Delivery staff are only granted access to the information necessary to support teaching, learning, and assessment activities. Aggregated or anonymised data may be used for reporting, analysis, and compliance purposes, but individual-level data is not shared beyond operational necessity.

Information flows are designed to ensure that data is only used for the purposes for which it was originally collected, and that any secondary use is assessed for compliance with data protection principles.

7. Data Sharing and Third Parties

Personal data is only shared where there is a lawful basis and a clear operational requirement to do so. This may include sharing data with funding bodies for audit and compliance purposes, awarding organisations for certification, and regulatory bodies where required by law.

Where third-party processors are used, the organisation ensures that appropriate contractual arrangements are in place in accordance with Article 28 of UK GDPR. These agreements require third parties to process data securely, confidentially, and only in accordance with documented instructions.

8. Data Security Measures

The organisation implements appropriate technical and organisational measures to ensure the security of personal data. These measures are designed to protect against unauthorised access, accidental loss, alteration, or disclosure.

Access to systems is controlled through role-based permissions, ensuring that staff only access data relevant to their role. Systems are protected using secure authentication methods, and data is stored on secure platforms with appropriate safeguards. Staff are required to complete mandatory training on data protection, information security, and confidentiality, and are expected to adhere to strict organisational policies at all times.

Security controls are regularly reviewed to ensure they remain effective and appropriate to the level of risk.

9. Data Retention and Disposal

Personal data is retained only for as long as is necessary to fulfil the purposes for which it was collected, including compliance with legal, regulatory, and funding requirements. Retention periods are determined based on statutory guidance and contractual obligations.

Learner records are typically retained for a minimum of six years following completion, in line with funding and audit requirements. Financial records are retained in accordance with tax and accounting legislation. Safeguarding records are retained in line with statutory safeguarding guidance and may be held for longer periods where required.

Once retention periods have expired, data is securely and permanently deleted or anonymised to prevent further identification.

10. Individual Rights

The organisation fully recognises and upholds the rights of individuals under UK GDPR. This includes the right to access personal data, request correction of inaccurate information, request erasure in certain circumstances, and object to processing where applicable. Individuals also have the right to request restriction of processing and data portability where conditions are met.

Requests are handled in accordance with statutory timeframes, typically within one calendar month, and are processed in a transparent and documented manner.

11. Consent

Where consent is used as a lawful basis for processing, it is obtained in a clear and transparent manner. Consent is specific to the processing activity, informed, and freely given, with individuals having the right to withdraw consent at any time.

Where consent is withdrawn, the organisation will cease processing the relevant data unless another lawful basis applies.

12. Data Breach Management

The organisation has established procedures for identifying, reporting, and managing personal data breaches. Any suspected breach is escalated immediately to the Managing Director for assessment and containment.

Where a breach is likely to result in a risk to individuals' rights and freedoms, it will be reported to the Information Commissioner's Office within 72 hours, in line with legal requirements. Affected individuals will also be informed where there is a high risk to their rights or privacy.

All breaches are recorded, investigated, and used to inform continuous improvement in data protection practices.

13. International Data Transfers

The organisation does not routinely transfer personal data outside the United Kingdom. Where international transfers are necessary, appropriate safeguards are implemented in accordance with UK GDPR requirements, such as adequacy regulations or approved contractual clauses.

14. Training and Compliance Monitoring

All staff receive training on data protection responsibilities as part of their induction and on an ongoing basis. Training ensures that staff understand how to handle personal data securely, recognise potential risks, and report incidents appropriately.

Compliance with this policy is monitored through internal audits, quality assurance processes, and periodic reviews of systems and procedures.

15. Policy Review

This policy is reviewed annually, or sooner where there are significant changes to legislation, systems, or organisational processes. Updates are approved by senior management to ensure continued compliance and effectiveness.