UK Professional Development Academy

Data Protection Policy

Data Protection Policy	Last Review:	January 2026
	Amended Date:	N/A
	Next planned review in 12 months, or sooner as required	

Data Protection Policy

1. Introduction

UK Professional Development Academy is committed to safeguarding personal data and ensuring compliance with data protection laws. The College needs to collect and process personal information about past, current, and prospective learners, employees, and stakeholders to function effectively and meet legal and regulatory obligations. Personal data must be collected and handled fairly, stored securely, and not disclosed unlawfully.

The College processes personal data for various purposes, including academic administration, assessment and certification, learner support services, financial transactions, compliance with statutory requirements, and operational management. Personal data held may include contact details, identification documents, assessment results, financial records, and health-related information where necessary.

Learners are responsible for ensuring that the personal data they provide to the College is accurate and up to date. Any changes to personal details, such as address or contact information, should be reported to the Student Office immediately. Learners should familiarize themselves with this policy, as failure to comply, whether deliberate or through negligence, may result in disciplinary action, withdrawal of access to College facilities, or legal consequences.

2. Scope

This policy applies to all learners, staff members, and stakeholders of UK Professional Development Academy. It ensures that all personal data held by the College is collected, processed, stored, and shared in compliance with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). The policy covers learner records, staff records, assessment data, financial transactions, and any other personal information held by the College.

3. Data Protection Principles

UK Professional Development Academy adheres to the seven key principles of data protection, as outlined in the UK GDPR:

1. **Lawfulness, fairness, and transparency** – Personal data is processed lawfully, fairly, and in a transparent manner.
2. **Purpose limitation** – Data is collected for specified, explicit, and legitimate purposes and not further processed in an incompatible way.
3. **Data minimization** – Only the data necessary for the intended purpose is collected and processed.

4. **Accuracy** – Reasonable steps are taken to ensure that personal data is accurate and kept up to date.
5. **Storage limitation** – Personal data is not kept longer than necessary for the specified purpose.
6. **Integrity and confidentiality** – Data is processed in a secure manner to prevent unauthorized access, loss, or destruction.
7. **Accountability** – The College takes responsibility for complying with data protection regulations and implementing appropriate measures.

4. Responsibilities for Data Protection

The Head of Quality is responsible for implementing this policy and ensuring compliance across the College. However, all staff, learners, and stakeholders are responsible for safeguarding personal data and adhering to data protection regulations.

Staff members must ensure that any personal data they provide to the College in connection with their employment is accurate and kept up to date. They must notify the College of any changes and ensure that data is used only for authorised purposes. Any data collected about others, such as learner coursework, references, or personal records, must be handled securely and not disclosed without appropriate authorisation. Any staff member who believes that this policy has been breached should report the matter to the Data Protection Officer. If the issue is not resolved, it may be raised as a formal grievance.

All learners must ensure that their personal data provided to the College is accurate and kept up to date. Changes in personal information, such as an updated address or contact details, should be reported to the Student Office as soon as possible. Learners using College IT systems may process personal data for coursework or research purposes and must ensure they comply with data protection regulations.

5. Data Security and Confidentiality

All staff and learners must ensure that personal data is stored securely and protected from unauthorised access or disclosure. Personal data held in physical form must be stored in locked filing cabinets or secure areas, while digital data must be protected with passwords and encryption. Unauthorised disclosure of personal data, whether intentional or accidental, may result in disciplinary action and, in serious cases, legal consequences.

Personal data should be accessed only by authorised individuals. Physical records should be kept in locked storage areas when not in use. Digital records should be stored on password-protected systems, with access granted only to those who require it. Any personal data shared externally must comply with data protection regulations and have the necessary permissions in place.

6. Rights of Data Subjects

Under the UK GDPR, individuals have rights regarding their personal data, including the right to access, rectify, erase, restrict processing, and object to the processing of their data. Learners and staff members may request a copy of their personal data held by the College by submitting a written request to the Data Protection Officer. The College will respond within one month unless an extension is required due to the complexity of the request.

If individuals believe that their personal data is inaccurate or incomplete, they have the right to request corrections. If there are legitimate grounds, they may also request that the College erase their data, restrict processing, or object to how their data is being used. However, certain legal or regulatory requirements may prevent the immediate deletion of specific records.

7. Data Sharing and Third-Party Access

Personal data may only be shared with third parties when there is a legal or regulatory obligation, such as sharing information with awarding bodies, funding agencies, or government departments. The College ensures that data shared with third parties is done securely and only when necessary. Any individual wishing to restrict how their data is shared should contact the Data Protection Officer.

8. Retention of Data

UK Professional Development Academy retains personal data only for as long as necessary to fulfil legal, regulatory, and operational requirements. Learner records are typically retained for six years after course completion, while financial and transactional records are kept for six years for audit and compliance purposes. Certification records are retained indefinitely for verification requests. Once data is no longer required, it is securely deleted or destroyed in compliance with data protection regulations.

9. Subject Consent and Processing of Sensitive Data

The College requires explicit consent to process sensitive personal data, including medical records, criminal convictions, or demographic data. Staff and learners may be required to provide additional information for health and safety reasons or to meet safeguarding requirements. The College will only use this information when necessary for operational, legal, or emergency purposes.

10. Breach Reporting and Incident Response

Any suspected data breach must be reported immediately to the Data Protection Officer. The College will investigate and take necessary action, including notifying affected individuals and,

where required, reporting the breach to the Information Commissioner's Office (ICO). Steps will be taken to prevent future breaches and improve data security measures.

Data Protection Notice

At UK Professional Development Academy, we are committed to protecting your personal data and handling it with transparency and care. This notice outlines how we collect, use, store, and protect your information in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. What Information We Collect

We collect personal data that you provide during your application and course of study, including:

- Name, date of birth, and contact details
- Identification documents
- Previous qualifications and work history
- Course progress, assessment results, and certificates
- Financial details for payments
- Health or support needs (if disclosed)

2. Why We Collect Your Data

We use your data to:

- Process applications and enrolment
- Manage your learning and assessment
- Issue certificates and communicate with awarding bodies
- Provide learner support and monitor progress
- Fulfil legal, regulatory, and audit obligations

3. Legal Basis for Processing

We process your data to fulfil our contract with you as a learner and to meet our legal obligations. Where required, we may ask for your consent.

4. How We Store and Protect Your Data

Your data is stored securely using password-protected systems and locked filing for physical records. Access is limited to authorised staff. We take all reasonable steps to prevent unauthorised access, loss, or misuse of your personal data.

5. Data Sharing

We may share your data with awarding bodies, funding agencies, or government authorities when required. We never sell your data or share it for marketing without your explicit consent.

6. Your Rights

You have the right to:

- Access the data we hold about you
- Request correction or deletion
- Object to or restrict processing
- Request a copy of your data in a portable format

Requests can be made in writing to our **Data Protection Officer** at:

Email: dpo@ukpdacademy.co.uk

Address: UK Professional Development Academy, First Floor, Fairlawn High Street, Southall, London

7. Retention of Data

We retain learner data for up to six years after course completion. Certification records may be held indefinitely to allow future verification.

8. Reporting Concerns

If you believe your data has been mishandled, you can contact our Data Protection Lead. You also have the right to lodge a complaint with the **Information Commissioner's Office (ICO)** at www.ico.org.uk.