Global-CPD Data Protection Policy

1. Purpose

This policy outlines how Global-CPD collects, stores, processes, and protects personal data in compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR). It ensures transparency, security, and respect for the privacy of all individuals whose data we handle.

2. Scope

This policy applies to:

- All personal data collected from CPD participants, partner institutions, trainers, and staff

- Data processed via online platforms, evaluation forms, registration documents, and communications

- All Global-CPD staff, trainers, consultants, and third-party service providers

3. Key Principles

Global-CPD commits to the following data protection principles:

- **Lawfulness, fairness, and transparency**: Data is collected and processed lawfully and transparently.

- **Purpose limitation**: Data is collected for specified, explicit, and legitimate purposes only.

- **Data minimisation**: Only relevant and necessary data is collected.

- **Accuracy**: Personal data is kept accurate and up to date.

- **Storage limitation**: Data is retained only as long as necessary.

- **Integrity and confidentiality**: Appropriate security measures are in place to protect personal data.

- **Accountability**: We maintain detailed records and conduct periodic reviews.

4. Data Collected

We may collect the following personal information:

- Names, contact details, job roles, institutional affiliation

- Participation and feedback data from training programs

- Evaluation responses and certification records

5. Use of Data

Collected data is used for:

- Registering and administering CPD programs

- Issuing certificates and maintaining learner records

- Evaluating program effectiveness

- Communicating with participants and partners

We do not sell, share, or rent personal data to third parties without explicit consent, except where legally required.

6. Data Storage and Security

All data is stored on secure servers or authorized cloud platforms with restricted access. Security measures include:

- Password protection and access control

- Encrypted storage where applicable

- Regular data backups

7. Rights of Data Subjects

Individuals have the right to:

- Access their data

- Request rectification or deletion

- Object to processing

- Withdraw consent at any time

- File a complaint with relevant data protection authorities

Requests must be sent in writing to **support@global-cpd.org** and will be responded to within 30 days.

8. Breach Notification

In case of a data breach, Global-CPD will assess the risk and, if necessary, notify affected individuals and the competent authorities within 72 hours, as required by law.

9. Policy Review

This policy is reviewed every **two years** by the Internal Quality Assurance Team or earlier if required by changes in delivery format, technology, or stakeholder needs.

For questions or concerns related to this policy, please contact:

Global-CPD Administrative Office
✉ Email: support@global-cpd.org
🌐 Website: www.global-cpd.org

Document Control

Policy Title: Data Protection Policy

Policy Reference: CPD-POL-04

Effective Date: 04.09.2008

Next Review Date: 04.05.2024

Version Number: V9.0

Policy Owner: Academic Coordinator, Global-CPD

Approval Authority: Director, Global-CPD

Status: Active

Revision History:

Version	Date	Author	Description / Changes
1.0	04.09.2008	Osman Bedel	Initial policy draft and approval
2.0	01.09.2010	QA Team	Defined categories of data collected
3.0	03.09.2012	QA Team	Introduced data subject access procedures
4.0	02.09.2014	QA Lead	Added data breach protocol
5.0	01.09.2016	Osman Bedel	Updated storage and access security details
6.0	03.09.2018	QA Team	Aligned fully with GDPR requirements
7.0	01.09.2020	QA Team	Clarified rights of data subjects and withdrawal of consent
8.0	02.09.2022	Policy Officer	Added cloud storage compliance and encryption measures
9.0	04.05.2024	Osman Bedel	Full revision and formatting under new Document Control