GDPR Compliance & Data Handling Policy

March 2024
CIFA GDPR Compliance Policy
Doc Number: OPS - GDPR
Version 2, 03/2025

1: Purpose of Compliant Storage in Excel

At CIFA Education Ltd, we are committed to ensuring the secure and compliant processing and storage of personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Our data handling processes align with the **Data Breach Policy (Doc Ref: DBP) and the Data Breach Plan and Procedures (Doc Ref: DPP)** to protect personal information, uphold individuals' rights, and meet legal requirements.

2: Identification and Understanding of Personal Data

We identify and categorise personal data contained in our reports, ensuring compliance with UK GDPR.

2.1: What is Personal Data?

Personal data refers to any information that can identify an individual, including:

- Name, email address and phone number
- Course enrolment details
- Payment information
- Complaints, feedback, screenshots and communications

2.2: What is Special Category Data?

Some personal data is considered more sensitive and requires additional protection, such as:

- Racial or ethnic origin
- Health information
- Biometric data
- Political opinions or religious beliefs

If a report contains personal data, we ensure full compliance with UK GDPR.

3: Legal Basis for Storing Data

All data storage activities have a lawful basis, including:

- Contractual Obligation – Retaining data to fulfil agreements with students and customers.
- Legal Obligation – Maintaining records to comply with UK tax, financial regulations and consumer protection laws.
- Legitimate Interest – Storing reports to enhance service quality and support audit procedures, ensuring it does not override individuals' rights. Please refer to the **Records Retention & Archiving Policy, Doc Ref: RRAP)**

4: Data Minimisation

4.1: Limiting Data Collection

- We only collect and retain necessary information for handling and auditing complaints, avoiding unnecessary personal details.

4.2: Anonymisation

- Where possible, we anonymise reports by removing or replacing personally identifiable information to enhance security and compliance.

5: Secure Storage Measures

To protect stored reports, we implement robust security controls. For details on the technical and cybersecurity measures implemented to protect personal data, refer to the **IT Security & Acceptable Use Policy, (Doc Ref: ITSAP)**. This policy outlines encryption protocols, access controls, and cybersecurity measures that align with UK GDPR compliance

5.1: Encryption

- All files containing personal data are encrypted to prevent unauthorised access.

5.2: Access Controls

- Only authorised personnel (audit team, managers) can access reports, with role-based permissions enforced.

5.3: Cloud Storage Compliance

- Cloud storage providers must comply with UK GDPR, ensuring data is stored within the UK or approved jurisdictions with adequate safeguards.

6: Retention and Deletion Policy

6.1: Retention Periods

- Customer complaint records are retained for six years to comply with UK consumer protection laws. Refer to our **Records Retention & Archiving Policy (Doc Ref: RRAP)**

6.2: Regular Audits

- Stored reports are periodically reviewed, and data exceeding the retention period is securely deleted or archived in line with the **Audit Plan and Procedures Manual. Refer to the Internal Audit Plan & Procedures Manual (Doc Ref: IAPP)**

7: Protecting Individual Rights

Under UK GDPR, individuals have the right to:

- Access – Request a copy of their data. Please refer to **(Appendix 1 SAR Form)**
- Rectification – Correct inaccuracies in stored data.
- Erasure – Request deletion of personal data where no legal basis exists for retention.
- Restriction – Request processing limitations on their data.

8: Incident Response Plan

We maintain a formal data breach response plan. Refer to the **Data Breach Plan and Procedure (Doc Ref: DBPP)**

- Any personal data breach is reported to the Information Commissioner's Office (ICO) within 72 hours.
- If a breach poses a high risk to individuals' rights and freedoms, affected individuals will be informed promptly.

9: Staff Training and Internal Policies

- Employees receive regular GDPR training to ensure compliance in handling, storing and securing reports.
- Internal policies govern data processing, report generation, access and deletion procedures to align with audit standards.

10: Documentation and Accountability

10.1: Record of Processing Activities (ROPA)

We maintain a **Record of Processing Activities, (Doc Ref: ROPA)**, detailing:

- Types of personal data stored.
- Security measures in place.
- Retention and deletion policies.
- The legal basis for data processing.

Appendix 1:

Subject Access Request (SAR) Form

CIFA Education Ltd – UK GDPR Compliance

1. Your Details

Full Name:

Address:

Postcode:

Email:

Phone Number:

Relationship to CIFA: Student ☐Former Student ☐ Employee ☐ Former Employee ☐ Other (please specify):

2. Details of Your Request

1. Please describe the personal data you are requesting access to:
   Course records, payment history, email communication or other:

2. Do you require data for a specific timeframe? (If yes, please specify dates)
   ☐ Yes, from to
   ☐ No, all relevant data

3. Please indicate the format in which you would like to receive your data:
   ☐ Email (secure PDF)
   ☐ Printed copy (by post)

3. Proof of Identity

We require **proof of identity** to protect your data before processing your request. Please provide a copy of **one** of the following:

- ☐ Passport
- ☐ Driving Licence
- ☐ Utility Bill (dated within the last 3 months)

4. Authorisation (if requesting on behalf of someone else)

If you are making this request on behalf of another individual, please provide:

Details:

Full Name of Data Subject:

Your Relationship	Parent/Guardian/Legal Representative
Evidence of Authority Submitted	☐ Signed Authorisation ☐ Power of Attorney ☐ Other (please specify):

5. Declaration

☐ I confirm that the information provided in this request is accurate. I understand that CIFA Education Ltd may need to contact me for further details and that my request will be processed within **one month** unless an extension is required.

Signature: _____

Date: / /

6. How to Submit Your Request

Send your completed form and proof of identity via:

Email: info@cifa.ac
Post: CIFA Education Ltd, 94-96 Seymour Place, London, W1H 1NB

7. What Happens Next?

- We will acknowledge your request within 5 working days.
- Your data will be provided within one month, unless your request is complex, in which case we may extend the deadline by up to two months.
- If we require additional information, we will contact you.

For further details, please review our section of our **GDPR Policy (Doc Ref: GDPR)** or contact our Compliance Officer via email: **eze@cifa.ac**