CIFA Risk Management Policy

Index

1. Introduction This Risk Management Policy aims to identify, assess and manage potential risks faced by CIFA Education Ltd, an online qualification awarding company in the education sector. The policy provides a structured framework for mitigating risks to ensure compliance with regulatory standards, safeguard data, maintain operational efficiency and uphold academic integrity.

2. Scope This policy applies to all areas of CIFA Education Ltd's operations, including governance, finance, academic delivery, compliance, IT security and student support. It also considers external relationships, including those with exam markers, tutors and partner organisations.

3. Risk Management Framework:

CIFA Education Ltd adopts a proactive approach to risk management through the following framework:

3.1 Risk Identification:

Key risk areas include:

- **Cybersecurity Risks:** Data breaches, cyberattacks and system vulnerabilities. Refer to the **IT Security & Acceptable Use Policy, (Doc Ref: ITSAP)**
- **Compliance and Regulatory Risks:** Non-compliance with GDPR and educational regulations, quality assurance failures. Refer to the **GDPR Policy (Doc Ref: GDPR)**
- **Operational Risks:** Technical failures, staffing shortages, reliance on third-party providers.
- **Reputation Risks:** Negative publicity, customer dissatisfaction. Refer to the **Complaints and Feedback Policy, (Doc Ref: CFP)**
- **Conflicts of Interest Risks:** External interests of markers, tutors, or authors affecting examination integrity. Employees engaging in private teaching related to our courses or examinations. Refer to the **Conflict of Interest Policy, (Doc Ref: COI)**

3.2 Risk Assessment:

Risks are evaluated based on the likelihood of impact and classified as Low, Medium, or High.

- **Cybersecurity Risks:** Moderate to high likelihood, severe impact.
- **Compliance and Regulatory Risks:** Moderate likelihood, severe consequences.
- **Operational Risks:** Moderate likelihood, variable impact.

- **Reputation Risks:** Moderate likelihood, significant impact on trust.
- **Conflicts of Interest Risks:** Managed through comprehensive internal and external monitoring. Refer to the **Conflict of Interest Policy, (Doc Ref: COI) and the Risk Assessment Process (Appendix 1 of COI Policy)**

3.3 Risk Mitigation Strategies:

- **Cybersecurity:** Implementation of robust security measures including Cloudflare protection, VPC networks, SHA256 password encryption, Ubuntu-based firewalls, DDOS protection, weekly backups and optional 2FA for students (mandatory for staff). Refer to the **IT Security & Acceptable Use Policy, (Doc Ref: ITSAP)** and the **Data Breach Plan and Procedure,(Doc Ref DBPP)**
- **Regulatory Compliance:** Continuous monitoring to ensure adherence to GDPR UK and educational best practices. Refer to the **GDPR Policy (Doc Ref: GDPR)**
- **Operational Resilience:** Investment in reliable IT infrastructure, redundancy systems and adequate staffing levels. Refer to the **Records Retention & Archiving Policy, (Doc Ref: RRAP)**
- **Reputation Management:** Transparent communication, proactive complaint handling and quality improvements. Refer to the **Complaints and Feedback Policy, (Doc Ref: CFP)**
- **Conflict of Interest Management:** Markers, tutors, or authors with external roles must declare potential conflicts. Risks are managed through rigorous internal and external monitoring. Refer to the **Conflict of Interest Policy (Doc Ref: COI)**

3.4 Monitoring and Review:

- Risks are reviewed periodically by the Compliance Officer and senior management.
- The CIFA Risk Management Report is used as a reference for ongoing risk evaluations.
- The risk register is updated regularly to reflect emerging risks.

- An annual risk management report is prepared for internal review. Refer to the **Organisational Policy for Handling Breaches & Monitoring Compliance (Doc Ref: OPHB)**

4. Roles and Responsibilities:

- **Senior Management:** Oversees risk management strategies and ensures compliance as per our Organisational Policy for Handling Breaches & Monitoring Compliance.
- **Compliance Officer:** Maintains the risk register, monitors compliance risks and recommends mitigation measures.
- **Staff Members:** Responsible for identifying and reporting risks within their roles. Refer to the **Organisational Policy for Handling Breaches & Monitoring Compliance, (Doc Ref: OPHB)**

5. Reporting and Escalation:

- Significant risks are reported to senior management for immediate action.
- Compliance-related risks that may affect regulatory approval are escalated to Ofqual if necessary.
- Internal audits evaluate the effectiveness of risk controls. Refer to the **Organisational Policy for Handling Breaches & Monitoring Compliance, Doc Ref: (OPHB)**

6. Policy Review:

This policy is reviewed annually or in response to significant regulatory changes. Updates are communicated to all relevant staff members and partners.