UK Professional Development Academy

Risk and Mitigation Policy and Contingency Plan

Risk and Mitigation Policy and Contingency Plan	Last Review:	January 2026
	Amended Date:	N/A
	Next planned review in 12 months, or sooner as required	

Risk and Mitigation Policy and Contingency Plan

1. Introduction

UK Professional Development Academy uses a structured approach to identify, assess, control and monitor risks that could affect learners, staff, quality, compliance, finances, information security or continuity of delivery.

2. Purpose

This policy establishes responsibilities, a consistent assessment method, escalation routes and contingency arrangements. It supports informed decision-making and timely action while recognising that not all risk can be eliminated.

3. Scope

The policy applies to strategic, operational, academic, financial, safeguarding, health and safety, information governance, cyber security, reputational and business continuity risks.

4. Risk Management Process

Risks will be identified, described and recorded in the risk register. Each risk will be scored for likelihood and impact on a scale of 1 to 5. The gross score reflects exposure before controls and the residual score reflects exposure after controls. Each risk must have an owner, controls, further actions, deadlines and a review date.

5. Risk Rating

Scores from 1 to 4 are low and managed through routine controls. Scores from 5 to 9 are moderate and require active monitoring. Scores from 10 to 15 are high and require senior management action. Scores from 16 to 25 are critical and require immediate escalation and a documented response.

6. Key Risks and Controls

UKPDA will maintain controls across the following areas:

Risk Area	Examples	Main Controls and Contingency Actions
Academic quality	Inconsistent assessment, low engagement, non-compliance	Qualified staff, standardisation, IQA sampling, learner support, corrective action plans
Assessment integrity	Plagiarism, impersonation, AI misuse, insecure materials	Authentication, learner declarations, secure access, investigations, awarding organisation notification
Information security	Cyber-attack, data loss, unauthorised access	Access controls, multi-factor authentication, backups, antivirus, incident response and recovery testing
Business continuity	LMS outage, premises loss, staff absence, utility failure	Alternative platforms, remote delivery, cross-trained staff, emergency contacts and backup records
Financial sustainability	Cash flow pressure, fraud, non-payment	Budgets, approvals, segregation of duties, debt control and regular review

Health, safety and safeguarding	Accident, welfare concern, unsafe practice	Risk assessments, reporting routes, trained staff, emergency procedures and referrals
Regulatory and awarding organisation	Missed requirements, adverse audit findings	Compliance calendar, policy review, staff training, internal audits and prompt reporting

7. Incident Response

When a significant event occurs, UKPDA will protect people first, contain the issue, preserve evidence, notify responsible managers, assess impact, communicate with relevant stakeholders, activate continuity arrangements and maintain an incident log. Statutory bodies and awarding organisations will be informed where required.

8. Business Continuity Priorities

Priority activities are learner communication, access to learning and assessment records, secure operation of the LMS, safeguarding response, payroll and finance, awarding organisation contact and recovery of critical data. Temporary arrangements must protect assessment validity and confidentiality.

9. Roles and Responsibilities

Senior management owns strategic and critical risks. The Quality Lead oversees academic and regulatory risks. The designated data protection and IT contacts manage information risks. Managers maintain local controls. All staff must report emerging risks, incidents and control failures promptly.

10. Monitoring and Reporting

The risk register will be reviewed at least quarterly and after significant incidents or change. High and critical risks will be reported to senior management. Lessons learned, actions and overdue controls will be tracked to closure.

11. Review and Testing

The policy and contingency arrangements will be reviewed annually. Backup restoration, contact lists, remote delivery arrangements and incident response processes will be tested periodically and after major system or organisational changes.