



BUSINESS CONTINUITY, CONTINGENCY AND DISASTER RECOVERY POLICY

Policy reference UKV-QA-03 | Version 3.0

UK Versity Online Limited | BAC Accredited College | UKPRN 10052768

Policy reference	UKV-QA-03
Version	3.0
Status	Consolidated
Effective date	1 October 2026
Next review	September 2027
Policy owner	Principal
Author	Director of Education
Approved by	Principal (Ramanjeet Singh), on behalf of the Academic Board
Approval date	1 October 2026

Business Continuity, Contingency and Disaster Recovery Policy

UK Versity Online Limited | ATHE 889 | Pearson 07737 | OTHM DC1506132 | Ascentis 3286 | NCFE 8465520 | IFA Direct 283334

Document control

Title	Business Continuity, Contingency and Disaster Recovery Policy
Reference	UKV-QA-03
Version	3.0
Status	Consolidated
Effective date	1 October 2026
Next review	September 2027 (annual), or earlier if required
Owner	Principal
Author	Director of Education
Approval authority	Academic Board, chaired by the Principal (Ramanjeet Singh)
Approval date	1 October 2026
Applies to	All UK Versity operations, systems, staff and learners, including NCFE Functional Skills external assessments conducted by the centre
Supersedes	Disaster Recovery Policy (QA-101, November 2014); Contingency Plan and Supporting Documentation (QA121, May 2024)
Summary	Sets out how UK Versity prepares for, responds to and recovers from events that disrupt teaching, assessment, learner records or operations, and how it protects learners and notifies awarding organisations.

Compliance mapping

BAC College Scheme 2023 standards	1.6; 2.7; 26.4
UK Quality Code 2024 (voluntary)	Principles 1, 3
OfS conditions (benchmark only; not OfS registered)	C3, C4 (benchmark)
Awarding organisations	ATHE; Pearson; OTHM; Ascentis; NCFE; IFA Direct
Legislation and regulation	UK GDPR and Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025); Health and Safety at Work etc. Act 1974; Management of Health and Safety at Work Regulations 1999; Ofqual General Conditions of Recognition

Version history

Version	Date	Change
1.0	November 2014	First issue as Disaster Recovery Policy (QA-101)

Version	Date	Change
2.0	May 2024	Contingency Plan and Supporting Documentation (QA121) issued for NCFE external assessments
3.0	October 2026	Full rebuild: business continuity, contingency and disaster recovery combined for an online college; NCFE external assessment contingency; awarding organisation notification; data breach link; BAC/QAA/OfS mapping and version control

1. Purpose

UK Versity Online Limited (trading as UK Versity) is a fully online distance learning college. Learners study on Moodle (lms.ukversity.co.uk) with live online tutor sessions, submit assignments electronically, and depend on UK Versity's systems for records, results and certification. NCFE Functional Skills learners sit external assessments conducted by the centre at UK Versity House, Salford.

This policy sets out how UK Versity:

- identifies and reduces the risks that could disrupt its service (BAC standard 1.6);
- responds to an incident quickly and in a controlled way;
- restores systems and data within set recovery times;
- protects learners' teaching, assessment and certification; and
- tells awarding organisations, regulators and learners what they need to know.

2. Scope

This policy covers all UK Versity operations, staff, contractors and systems, and all learners on qualifications from ATHE (Awarding body for Training and Higher Education), Pearson Education Ltd (Pearson BTEC, including BTEC Higher Nationals), OTHM Qualifications, Ascentis (including Access to HE Diplomas, validated under the QAA Access to HE scheme), NCFE (including qualifications under the NCFE CACHE brand, and NCFE Functional Skills) and Institute of Financial Accountants (IFA) qualifications delivered through IFA Direct, administered in partnership with ATHE.

For learners on Pearson BTEC Higher National programmes, the Pearson HN edition of this policy (v3.0, July 2026) applies and takes precedence where the two differ.

Where an event leads to UK Versity withdrawing a qualification, losing centre approval or ceasing to trade, the Learner Protection and Qualification Withdrawal Policy (UKV-QA-04) also applies.

3. Definitions

- **Incident:** any event that disrupts, or threatens to disrupt, teaching, assessment, learner support, records or UK Versity's operation.
- **Business continuity:** keeping essential services running, or restoring them quickly, during and after an incident.
- **Disaster recovery:** restoring IT systems and data after a failure, attack or loss.
- **Recovery Time Objective (RTO):** the maximum time a system may be unavailable before it must be restored.
- **Recovery Point Objective (RPO):** the maximum period of data that may be lost, measured back from the incident.
- **Incident Management Team (IMT):** the group that leads the response (section 6).

4. Policy statement and principles

1. Learners come first. In any incident UK Versity acts to protect learners' safety, their assessment and their records.
2. UK Versity keeps a written Business Continuity Risk Register and Business Continuity Plan, reviewed at least twice a year and after every significant incident.
3. Critical data is backed up daily and can be restored within the RTOs in section 7.
4. Every key role has a named deputy, recorded in the Business Continuity Plan.
5. Awarding organisations are told promptly about any event that could affect learners, assessment or certificates (section 9).
6. Personal data breaches are handled under the Data Protection and Records Retention Policy (UKV-QA-29).
7. Plans are tested at least once a year.

5. Risk assessment

The Principal keeps the Business Continuity Risk Register. Each risk is scored for likelihood and impact, with an owner and controls. The main risks for UK Versity as an online college are:

Risk	Main controls
Moodle unavailable (hosting failure, update fault)	Dedicated cloud server with hosting provider ENIX Ltd; daily backups with a copy held on Dropbox; hosting provider support; staff access to cPanel server management
Zoho services unavailable (CRM, Mail, WorkDrive)	Provider resilience; exports of key learner and registration data; alternative contact through Moodle and telephone
Microsoft or Zoom unavailable	Live sessions can move between Zoom and Microsoft Teams; sessions are recorded and uploaded to Moodle
Cyber incident (ransomware, phishing, account compromise)	Multi-factor authentication on key accounts, access controls, staff awareness training, software updates, isolation procedure
Personal data breach	UKV-QA-29 procedure; breach log; 72-hour ICO reporting
Loss of key staff	Named deputies; written procedures; shared mailboxes; cross-training
Loss of the Salford office	Staff can work remotely; records held in the cloud; certificates stored securely with a recorded alternative dispatch arrangement
Awarding organisation withdraws a qualification or centre approval	UKV-QA-04 teach-out and transfer arrangements
Disruption to NCFE Functional Skills external assessments	Contingency plan and evacuation procedure in section 8
Pandemic or public health restrictions	Fully online delivery already in place; remote working for staff
Financial or supplier failure	Senior Management Team financial monitoring; supplier review

6. Incident response

6.1 Incident Management Team

The IMT is led by the Principal and Director of Education. Members are the Quality Manager, the Centre Coordinator and the Financial Controller (the Senior Management Team), joined as needed by the Registrar, the Examinations Officer and NCFE Coordinator, the Course Coordinator and the Designated Safeguarding Lead. If the Principal is unavailable, the Quality Manager leads.

6.2 Incident levels

Level	Description	Response
1. Minor	Short disruption to one service, no effect on assessment or data (for example Zoom failure for one session)	System owner resolves; logs the incident
2. Significant	Disruption to a Tier 1 or Tier 2 system, or to an assessment, or any suspected data breach	IMT convened within 2 hours; learners and awarding organisations informed as needed
3. Major	Prolonged loss of Moodle or learner records, serious cyber incident, loss of key staff, loss of centre approval, or any event threatening UK Versity's ability to continue	IMT convened immediately; Business Continuity Plan and, where relevant, UKV-QA-04 invoked

6.3 Response steps

1. **Report.** Any member of staff who becomes aware of an incident reports it at once to their line manager and the Centre Coordinator. Suspected data breaches and cyber incidents are reported immediately to the Data Protection Lead.
2. **Contain.** The system owner acts to stop the harm spreading. For a cyber incident this includes disconnecting affected devices from the network, changing compromised passwords and contacting the hosting provider.
3. **Assess.** The IMT decides the incident level, the systems and learners affected, whether personal data is involved and whether any assessment or certification is affected.
4. **Communicate.** The IMT agrees messages for staff, learners, awarding organisations and, where needed, the ICO, BAC and insurers (section 10).
5. **Recover.** Systems are restored from backup or switched to alternatives, in RTO order (section 7). Data integrity is checked before normal use resumes.
6. **Protect learners.** Deadlines are extended where learners have been disadvantaged, and special consideration is applied under UKV-QA-18 where an assessment is affected.
7. **Record.** Every action and decision is logged with the time and the person responsible.
8. **Review.** A post-incident review is completed within 10 working days of recovery (section 11).

7. Disaster recovery: systems, backups and recovery times

7.1 System tiers

System	Tier	RTO	RPO	System owner
Moodle (learning platform, assignment submissions, feedback)	1	4 hours	1 hour	Course Coordinator

System	Tier	RTO	RPO	System owner
Learner records, registration and assessment records	1	4 hours	1 hour	Registrar
Email and CRM (Zoho)	2	24 hours	4 hours	Centre Coordinator
Finance and payments	2	24 hours	4 hours	Financial Controller
Live session platforms (Zoom, Microsoft Teams)	2	24 hours	Not applicable	Tutor Coordinator
File storage and archives (Zoho WorkDrive)	3	72 hours	24 hours	Centre Coordinator

7.2 Backups

- Critical data is backed up daily (incremental) and weekly (full).
- Backups are held off the primary system: the Moodle server is backed up by the hosting provider and a further copy is held on Dropbox; assessment and internal quality assurance records are archived electronically on Zoho WorkDrive with access controls.
- Backup integrity is checked monthly by restoring a sample file.
- Third-party providers must hold their own disaster recovery arrangements. The Centre Coordinator checks these when a contract starts and at renewal.

7.3 Alternative arrangements

If Moodle is unavailable for more than 4 hours, learners are told by email how to submit work (learnerwork@ukversity.co.uk) and all submission deadlines falling during the outage are extended by at least the length of the outage. If email is unavailable, UK Versity uses Moodle announcements, the website and telephone (0161 273 4745).

8. NCFE Functional Skills external assessments: contingency plan

NCFE's Regulations for the Conduct of External Assessments require the centre to have an external assessment contingency plan and an emergency evacuation procedure. This section is that plan. It is applied with the Examinations and Controlled Assessment Policy (UKV-QA-22) and UKV-NCFE-FS-P-01 Plagiarism, Malpractice and Examination Conduct Policy v1.0 (18 September 2026), which applies to NCFE Functional Skills external assessments.

Disruption	Action	Responsible
Fire alarm or evacuation	Candidates leave all papers and equipment on the desk and remain under examination conditions. They do not communicate and are supervised at all times on the way to and at the assembly point (in front of the building, Carrol Grove Street side). The invigilator records the time of leaving and returning. If it is safe to resume, the remaining time is given.	Invigilator; Examinations Officer
Power failure	Candidates stay seated under examination conditions. The invigilator contacts NCFE customer support. If power is not restored within 15 minutes, the session is stopped and rescheduled with NCFE.	Invigilator; Examinations Officer

Disruption	Action	Responsible
On-screen system or hardware failure	The invigilator contacts NCFE customer support. Timing is reset and the candidate re-admitted to previous responses where NCFE permits and it is technically possible. Otherwise the assessment is rescheduled.	Invigilator; Examinations Officer
Candidate illness or emergency	First aid and, if needed, 999. The candidate's assessment is ended or paused as NCFE rules allow; special consideration is considered.	Invigilator; Examinations Officer
Invigilator unavailable	A trained reserve invigilator from the Invigilator Register takes over. If none is available, the session is rescheduled before it starts.	Examinations Officer
Office unavailable on the assessment day	Candidates are contacted by telephone and email and the session is rescheduled with NCFE.	Examinations Officer
Suspected breach of assessment security	Handled as suspected malpractice under UKV-NCFE-FS-P-01 and reported to NCFE immediately.	Examinations Officer; Quality Manager

Every disruption is recorded on an incident report, reported to NCFE with full details, and kept with the assessment records. Learners affected are told in writing of the next steps within 2 working days.

9. Notifying awarding organisations

Under the Ofqual General Conditions of Recognition, awarding organisations must tell Ofqual about events that could have an adverse effect on learners or on the qualifications they award. They rely on their centres to tell them promptly. UK Versity will therefore notify the affected awarding organisation(s), by the route set out in each centre agreement, on the same or next working day after it becomes aware of any event that could:

- prevent learners from being taught or assessed, or delay their results or certificates;
- compromise the security or integrity of assessment materials, learner work or assessment records;
- involve the loss, corruption or unauthorised disclosure of learner data held for the awarding organisation;
- affect UK Versity's ability to meet its centre approval conditions, including loss of key staff such as the Head of Centre, the Quality Manager or the Examinations Officer.

The Centre Coordinator makes the notification for ATHE and IFA Direct, the Examinations Officer and NCFE Coordinator for NCFE, and the Registrar for Pearson, OTHM and Ascentis, each copying the Principal. Suspected malpractice or maladministration is reported under the Malpractice and Maladministration Policy and Procedure (UKV-QA-20).

10. Communication

- **Learners:** Moodle announcement and email as soon as the scale of disruption is known, with updates at least every working day until service is restored. Messages say what has happened, what learners need to do, and any change to deadlines.
- **Staff:** email or telephone from the IMT lead.
- **Awarding organisations:** as section 9.

- **Information Commissioner's Office:** a personal data breach that is likely to result in a risk to individuals is reported to the ICO within 72 hours of UK Versity becoming aware of it, under UKV-QA-29. Where the risk to individuals is high, they are told without undue delay.
- **BAC:** informed of any major incident affecting UK Versity's ability to meet the accreditation standards.
- **Insurers and police:** informed where required, for example after a cyber attack or theft.

11. Post-incident review and testing

After every Level 2 or Level 3 incident, the IMT lead completes a post-incident review within 10 working days. It records the cause, the timeline, what worked, what did not, the effect on learners, and actions. The Business Continuity Risk Register and Plan are updated.

Each year, the Principal arranges:

1. a scenario (desk-top) exercise with the IMT, covering at least one systems scenario and one staffing or approval scenario;
2. a test restore of Moodle and learner records from backup, timed against the RTOs;
3. a fire evacuation drill at UK Versity House, and a briefing for invigilators on the external assessment contingency plan in section 8.

Test results and actions are recorded and reported to the Academic Board.

12. Roles and responsibilities

Role	Responsibility
Principal and Director of Education	Owns this policy; leads the IMT; keeps the Business Continuity Risk Register and Plan; decides when UKV-QA-04 is invoked; arranges annual testing
Quality Manager	Deputy IMT lead; protects assessment and IQA records; applies special consideration and assessment arrangements after disruption
Centre Coordinator	Logs incidents; manages suppliers and hosting provider; owns email, CRM and file storage recovery; notifies ATHE, IFA Direct and BAC
Financial Controller	Owns finance system recovery; insurance; financial risk monitoring
Registrar	Owns learner and registration records recovery; notifies Pearson, OTHM and Ascentis
Examinations Officer and NCFE Coordinator	Applies the external assessment contingency plan; notifies NCFE; keeps incident reports
Course Coordinator	Owns Moodle recovery and learner communications on Moodle
Tutor Coordinator	Moves live sessions to alternative platforms; arranges tutor cover
Data Protection Lead	Leads the response to any personal data breach, including ICO reporting
Designated Safeguarding Lead	Advises on any welfare or safeguarding effect of an incident
All staff	Report incidents immediately; follow IMT instructions

13. Awarding organisation requirements

AO	Requirement / escalation route	Source document
NCFE	External assessment contingency plan and emergency evacuation procedure; disruption and suspected malpractice reported to NCFE	NCFE Regulations for the Conduct of External Assessments; NCFE Malpractice and Maladministration Policy PA-014 v1.1
Pearson	Pearson BTEC Higher Nationals: the Pearson HN edition applies; records remain available to Pearson during and after any continuity event	Disaster Recovery Policy (Pearson HN) v3.0, July 2026
ATHE	Tell ATHE promptly of events affecting learners or assessment; malpractice reported within 5 working days of discovery	ATHE centre agreement; ATHE Malpractice and Maladministration Policy, 2023
OTHM	Tell OTHM promptly of events affecting learners or assessment; malpractice reported promptly	OTHM centre agreement; OTHM Malpractice, Maladministration and Investigations Policy v4.1, August 2026
Ascentis	Tell Ascentis promptly of events affecting learners or assessment	Ascentis Centre Agreement, April 2026
IFA Direct	Notified through the ATHE route	ATHE centre agreement

14. Related policies and legislation

- UKV-QA-01 Quality Assurance Framework and Policy Governance Policy
- UKV-QA-04 Learner Protection and Qualification Withdrawal Policy
- UKV-QA-13 Online and Distance Learning and Course Materials Policy
- UKV-QA-18 Reasonable Adjustments, Special Consideration and Mitigating Circumstances Policy
- UKV-QA-20 Malpractice and Maladministration Policy and Procedure
- UKV-QA-22 Examinations and Controlled Assessment Policy
- UKV-QA-29 Data Protection and Records Retention Policy
- UKV-QA-30 Acceptable Use, E-Safety, Email and Social Media Policy
- UKV-QA-31 Health, Safety and Wellbeing Policy
- UKV-NCFE-FS-P-01 Plagiarism, Malpractice and Examination Conduct Policy v1.0 (18 September 2026)
- UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
- Health and Safety at Work etc. Act 1974; Management of Health and Safety at Work Regulations 1999
- Ofqual General Conditions of Recognition
- BAC College Scheme 2023, standards 1.6, 2.7 and 26.4
- QAA UK Quality Code for Higher Education (2024), Principles 1 and 3
- OfS conditions C3 and C4, used as voluntary benchmarks only

15. Monitoring and review

The Principal reports to the Academic Board at least annually on incidents, post-incident reviews, test results and changes to the risk register. The Senior Management Team reviews the Business Continuity Risk Register at least twice a year.

This policy is reviewed at least annually, and earlier if legislation, awarding organisation requirements, BAC standards, an EQA or inspection action, or a significant incident requires it. Incident logs, post-incident reviews and test records are kept for at least 3 years; records linked to a personal data breach are kept as set out in UKV-QA-29.

Approval and review

Stage	Name and role	Date
Prepared by	Director of Education	30 September 2026
Checked by (policy owner)	Principal	30 September 2026
Approved by	Ramanjeet Singh, Principal and Director of Education, on behalf of the Academic Board	1 October 2026
Next review due	Quality Manager (Shazia Khan) to schedule through the Policy Register UKV-QA-REG	September 2027