

## Examinations Contingency Plan

### Examinations Centre

|                         |                                                                  |
|-------------------------|------------------------------------------------------------------|
| <b>Centre</b>           | Excel Tutors (Centre 10488)                                      |
| <b>Address</b>          | 161-163 Commercial Road, London, E1 2DA                          |
| <b>Policy owner</b>     | Head of Centre                                                   |
| <b>Operational lead</b> | Exams Officer                                                    |
| <b>Last reviewed</b>    | July 2026                                                        |
| <b>Review cycle</b>     | Annually, on publication of updated JCQ regulations and guidance |

### This policy is aligned with:

- JCQ General Regulations for Approved Centres 2025-2026
- JCQ Instructions for Conducting Examinations 2025-2026
- JCQ Exam system contingency plan (Ofqual/JCQ) 2025-2026

*Reviewed annually on the publication of updated JCQ regulations and guidance (General Regulations for Approved Centres, Instructions for Conducting Examinations, and related documents).*

---

## Excel Tutors, Examinations Contingency Plan (2025 Edition)

This plan sets out how Excel Tutors Examination Centre will prepare for, respond to, and recover from disruptions to examinations and assessments. It aligns with JCQ 'General Regulations', JCQ 'Instructions for Conducting Examinations (ICE)', Ofqual conditions, CCEA guidelines, UK GDPR and the Data Protection Act 2018.

### 1. Purpose, Scope and Principles

**Purpose:** Ensure examinations/assessments proceed with integrity, fairness and compliance during planned and unplanned disruptions; minimise risk to candidates; and maintain timely, accurate communication with awarding bodies and stakeholders.

**Scope:** Applies to all qualifications delivered by the Centre (GCSE, AS/A level, Functional Skills and any vocational equivalents), and to all assessment types (written exams, on-screen tests, NEA/coursework, practicals, speaking/listening, controlled assessments).

Principles: (i) Compliance first; (ii) Candidate safety and welfare; (iii) Integrity of assessment; (iv) Data security; (v) Proportionality and documented decision-making; (vi) Clear accountability; (vii) Timely escalation and communication; (viii) Post-incident review and learning.

## 2. Roles, Responsibilities and Deputies

**Head of Centre (HoC):** Overall accountability for regulatory compliance; declares the Centre 'exam ready'; authorises contingency activation; liaises with regulators/awarding bodies at senior level; approves alternative sites and timetable variations; signs incident reports.

**Exams Officer (EO):** Operational lead for delivery; maintains exam timetable; secures question papers/scripts; activates invigilation cover; coordinates rooming/IT; communicates with awarding bodies regarding entries, special consideration, late arrivals, and script dispatch; maintains incident log.

**Data Protection Lead (DPL):** Advises on UK GDPR/DPA 2018 compliance; ensures secure handling of candidate/staff data during incidents; oversees breach assessments and ICO notifications; controls access to digital systems and backups; records data processing decisions.

**SENCo/Access Arrangements Lead:** Ensures reasonable adjustments and AAs are maintained during disruptions; arranges alternative rooms/technology and additional supervision.

**IT Lead:** Ensures availability of on-screen testing platforms, network, power continuity, printing/scanning; executes cyber-incident playbooks; maintains offline/backup solutions.

**Site/Facilities Manager:** Ensures room readiness, health & safety, emergency evacuation, alternative site setup, physical security; manages severe weather and building issues.

**Lead Invigilator:** Implements ICE in the room; manages candidate movement, late arrivals, emergencies; completes incident forms and statements; preserves evidence.

**Safeguarding Lead:** Assesses welfare risks during extended disruptions/evacuations; coordinates supervision; records safeguarding concerns and escalations.

**Deputies:** Each role must nominate at least one trained deputy recorded in the Centre's Exams Contact List (Appendix A). Deputies have delegated authority when the role holder is unavailable.

## 3. Triggers for Activating this Plan

The Plan may be activated when a disruption threatens exam integrity, candidate access, compliance or safety, including (but not limited to): severe weather, transport disruption, staff absence, building issues, IT/cyber incidents, power outages, security breaches, loss/compromise of papers, late paper delivery, awarding-body system outages, emergency evacuations, public health restrictions, or incidents affecting a large cohort or key personnel.

## 4. Risk Register, Key Scenarios and Responses

### 4.1 Severe Weather / Transport Disruption

- Decision: HoC/EO assess feasibility to proceed safely. Consider delayed start within JCQ parameters; alternative site usage; or reschedule in coordination with awarding bodies.
- Actions: Communicate arrival guidance to candidates; deploy additional invigilators for staggered starts; record late arrivals; apply special consideration where appropriate; preserve exam security during delays.
- Evidence: Attendance records, travel disruption evidence, invigilator statements, communications log.

### 4.2 Significant Staff Absence (Invigilators/EO/HoC)

- Decision: Activate invigilator reserve list and agency cover; deploy trained deputies for EO/HoC.
- Actions: Prioritise high-risk sessions (large cohorts, on-screen); re-room to consolidate supervision; ensure ICE ratios; brief cover staff; document deviations authorised by HoC.
- Evidence: Rota, training records, incident forms.

### 4.3 Centre Closure / Loss of Premises

- Decision: HoC activates alternative approved venue (Appendix B).
- Actions: Secure transport of exam materials; update signage and candidate communications; coordinate site readiness (H&S, accessibility, clocks, posters, seating, secure storage).
- Evidence: Chain-of-custody for papers/scripts; photos; venue hire agreement; room plans.

### 4.4 Loss/Delay/Compromise of Question Papers or Secure Materials

- Decision: Treat as a security breach. EO isolates affected materials; HoC informs awarding body immediately.
- Actions: Do not use compromised materials; follow awarding-body instructions for replacements; complete security incident report; preserve CCTV/access logs.
- Evidence: Secure storage access logs, courier records, statements, awarding-body correspondence.

### 4.5 Emergency Evacuation / Invacuation / Lockdown

- Decision: Lead Invigilator initiates emergency procedure; EO/HoC informs awarding body if assessment integrity is at risk.
- Actions: Stop exam; instruct candidates to close scripts face-down; evacuate per safety routes; maintain silence and supervision; do not allow discussion; note timings; resume if

safe, adjusting end time; if not feasible, seek awarding-body guidance for partial completion/special consideration.

- Evidence: Fire log, timings, invigilator statements, candidate seating plan annotations.

#### 4.6 IT Failure / On-Screen Testing Platform Outage

- Decision: IT Lead evaluates local vs. platform-wide issue; HoC/EO decide on delay, switch to backup devices, or reschedule.
- Actions: Switch to offline/backup test mode if permitted; rotate cohorts; ensure autosave/recovery protocols; log affected candidates and timestamps; report to awarding body and platform provider.
- Evidence: Incident tickets, screenshots, provider status updates.

#### 4.7 Power Outage

- Decision: Assess duration; if brief, pause and extend; if prolonged, move to rooms with natural light or alternative site.
- Actions: Protect integrity of on-screen tests; secure scripts; monitor environment conditions; communicate revised timings.
- Evidence: Utility provider confirmation, timing records.

#### 4.8 Cyber Incident (Malware, Phishing, Ransomware)

- Decision: Activate IT cyber playbook; isolate affected systems; DPL assesses personal-data risk.
- Actions: Switch to paper-based processes where safe; use clean devices; inform awarding bodies of any compromised data transmission; consider ICO notification within 72 hours if risk to individuals.
- Evidence: Forensic logs, IOC lists, breach assessment, communications.

#### 4.9 Misuse of AI / Academic Integrity Concerns (NEA/Remote Prep)

- Decision: EO/SENCo/Subject Lead assess authenticity; follow malpractice policy.
- Actions: Use approved tools for authorship checks where permitted; obtain candidate declarations; retain drafts/version history; refer suspected cases to awarding body.
- Evidence: Plagiarism/AI-use reports, witness statements, candidate declarations.

#### 4.10 Illness, Injury, Distress or Bereavement

- Decision: Safeguarding Lead advises; consider rest breaks, room changes, or withdrawal.
- Actions: Provide supervision; record details; apply for special consideration with evidence; ensure first aid and welfare support.

- Evidence: First-aid records, communications with parents/carers, medical notes where applicable.

#### 4.11 Late Arrival / Very Late Arrival

- Decision: Admit per JCQ rules where feasible without compromising security.
- Actions: Seat candidate separately; supervise; adjust end time; if very late, confirm paper security before admission; file report to awarding body.
- Evidence: Arrival times, supervision record, candidate statement.

#### 4.12 Awarding-Body System Outage / Courier Failure

- Decision: Use alternative submission windows; arrange contingency collections/deliveries.
- Actions: Maintain secure storage; track all attempts; keep awarding body informed; escalate through senior contacts if deadlines at risk.
- Evidence: Email chains, ticket numbers, courier logs.

### 5. Command, Control and Communication (C3)

Activation: HoC (or deputy) declares incident level (Minor, Significant, Major) and activates the Contingency Plan. EO opens the Incident Log (Appendix C).

Incident Team: HoC (Gold), EO/IT/Site/Safeguarding (Silver), Invigilation/Room Leads (Bronze).

Communication Priorities: (1) Safety; (2) Exam integrity; (3) Awarding body notifications; (4) Candidate/parent comms; (5) Staff and site operations; (6) External partners (transport, venue, IT).

Channels: SMS broadcast, email, website/portal banner, centre phone line update, on-site notices, social media (where approved). All outbound communications must be concise, factual, and avoid sensitive details. DPL to review messages where personal data is included.

### 6. Delivery Adjustments and Alternative Arrangements

Permissible adjustments must follow awarding-body guidance and ICE. Options include delayed start, supervised isolation, alternative accommodation/venue, split cohorts, rescheduling with approval, modified rooming, additional invigilation, and, where explicitly permitted, use of backups for on-screen tests. All adjustments require documented justification and authorisation by HoC/EO.

### 7. Secure Materials Management

Secure receipt, storage and distribution of question papers and materials will follow JCQ ICE. During incidents, security controls are tightened: dual-person access to secure room; real-time access log; tamper-evident packaging; chain-of-custody records; CCTV review (if available);

immediate isolation of any suspect packages/materials. Script dispatch follows awarding-body requirements with contingency for courier failures.

## 8. Data Protection, Records and Evidence

All records created during an incident are personal data and must comply with UK GDPR/DPA 2018. The DPL ensures minimal disclosure, secure storage, and role-based access. Evidence may include emails, logs, screenshots, photos, statements, and CCTV. Retention: incident logs and reports kept for 6 years (or awarding-body requirement if longer). Breach assessments completed within 72 hours where applicable; consider ICO notification.

## 9. Special Consideration and Post-Incident Support

EO coordinates special consideration applications with evidence (attendance, medical notes, travel disruption proof, invigilator statements). Welfare support offered via Safeguarding Lead. Candidates and staff receive clear information about outcomes, next steps, and appeals routes.

## 10. Recovery and Resumption

Following stabilisation, the Centre prioritises backlog processing (entries, script dispatch, results queries), reconciles any timetable changes, and restores normal operations. IT performs root-cause remediation and hardening. Facilities complete repairs and safety checks. EO finalises incident report with timeline, decisions, approvals, and evidence catalogue.

## 11. Testing, Training and Review

Training: Annual training for EO, invigilators, IT, site and senior leaders on this Plan and JCQ/ICE updates; induction for new staff; tabletop exercises each term covering at least one Major scenario; practical drill annually (evacuation or IT outage).

Review: Plan reviewed each year (or after any significant incident) by HoC with input from EO, DPL, IT, Site and Safeguarding. Changes are version-controlled and communicated to staff. Latest signed version stored in the secure Exams folder and shared with awarding bodies on request.

## 12. Equality, Diversity and Inclusion

All contingency decisions will consider the impact on candidates with disabilities or additional needs and those with protected characteristics. The SENCo ensures reasonable adjustments remain effective during any alternative arrangements.

## 13. Insurance and Financial Considerations

The Centre maintains appropriate insurance. Where incidents incur costs (alternative venue, couriers, additional staffing), EO/Site Manager record cost codes; HoC authorises claims and budget variances.

## Appendix A, Exams Contact List (Role-Based)

Populate and keep current. Store personal phone numbers securely (UK GDPR).

- Head of Centre (HoC): \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- Exams Officer (EO): \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- Deputy EO: \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- Data Protection Lead (DPL): \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- IT Lead: \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- Site/Facilities Manager: \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- Safeguarding Lead: \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- SENCo/AA Lead: \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- Alternative Venue Manager: \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_
- Awarding Body (General enquiries): \_\_\_\_\_ Phone: \_\_\_\_\_ Email: \_\_\_\_\_

## Appendix B, Pre-Approved Alternative Venues

List venue details, capacity, accessibility, secure storage options, travel directions, and contact names. Site Manager to inspect annually and record H&S compliance.

Venue 1: \_\_\_\_\_ Capacity: \_\_\_\_\_ Secure storage: Yes/No Accessibility: Yes/No  
Notes: \_\_\_\_\_

Venue 2: \_\_\_\_\_ Capacity: \_\_\_\_\_ Secure storage: Yes/No Accessibility: Yes/No  
Notes: \_\_\_\_\_

## Appendix C, Incident Log Template

Use one log per incident; keep sequential page numbers; store in secure Exams folder.

1. Incident title and ID
2. Date/time opened and closed
3. Location(s)
4. People involved (roles only in log; personal details in secure annex)
5. Description and trigger
6. Immediate actions taken (with timestamps)
7. Decisions, approvals and authorising role

8. Awarding-body notifications (ref numbers)
9. Candidate impact (numbers, identifiers)
10. Data protection considerations (breach? SAR risk?)
11. Evidence catalogue (attachments list)
12. Next actions and owners
13. Post-incident review outcomes

## Appendix D, Communications Matrix and Templates

Matrix: who to tell, when, how, and owner of message.

- Awarding body, Immediately for security/serious incidents, EO/HoC, Phone + email confirmation.
- Candidates, As soon as safe and clear, EO, SMS/email/website banner.
- Parents/Carers, Where appropriate, EO/Safeguarding, Email/SMS.
- Staff/Invigilators, Immediately, EO, Briefing sheet + WhatsApp/Teams channel (if approved).
- IT/Facilities, Immediately for technical/site issues, IT Lead/Site Manager, Ticketing system + phone.
- Emergency Services, Immediately if safety risk, HoC/Site - 999 + incident number recorded.

Template, Candidate Message (delay):

'Your exam in [subject] scheduled for [date/time] will start later due to [reason]. Please aim to arrive by [new time]. Follow staff instructions on arrival. Do not discuss the paper. Bring your ID. We will keep you informed.'

Template, Awarding Body Message (security):

'We have identified a potential security compromise affecting [paper/code]. The materials are isolated; no candidates have seen them. Requesting guidance on replacements and reporting requirements. Incident ID: [ID]. Contact: [name/role/number].'

## Appendix E, Checklists

E1: Activation Checklist

- Confirm trigger and level; ensure safety first.
- Appoint Incident Lead (HoC or deputy).



- Open Incident Log (Appendix C) and unique ID.
- Secure materials and rooms; confirm headcount and invigilator cover.
- Notify awarding body if required; obtain instructions.
- Issue stakeholder communications (Appendix D).
- Confirm data protection controls; restrict access to need-to-know.

#### E2: Recovery Checklist

- Reconcile timings, attendance and adjustments; update seating plans.
- Dispatch scripts or upload responses per instructions.
- Raise special consideration requests with evidence.
- Restore IT/services; collect logs and screenshots.
- Complete incident report and evidence pack.
- Hold hot debrief; schedule formal review; update training and Plan.