ETC International College

Contingency and Adverse Events Policy

Jan 2026

Contents:

1.0 Scope and Purpose:

1.1 This policy defines the policy, processes and procedures of ETC International College with respect to unforeseen incidences and events that seriously impact delivery of contracted college services (principally, the teaching of courses to enrolled students).

1.2 A contingency plan is a routinely updated plan for responding to a system emergency that includes performing backups, preparing critical facilities, and appropriately detailed migration plans that can be used to facilitate continuity of operations in the event of an emergency and recovering from a disaster.

1.3

1.4 By outlining actions/procedures to be invoked in case of disruption it is intended to mitigate the impact these disruptions have on the business, staff, students and clients of ETC International College.

1.5 The following policies and documents refer to specific events and form a part of the college's overall contingency plans:

- ETC International College Procedure: Response to Major Incidents (including Terrorist / Firearms / Weapons Attack and Bomb Threats); current issue.
- Exams Contingency Procedure, current issue.
- Student Protection Plan, current issue (section 1 "ETC is no longer able to operate"; "ETC is no longer able to deliver courses in one or more subject areas due to inaccessible premises").
- Documentation Retention and Secure Storage Policy, current issue (section 4.0 "Preventing Damage, Theft or Loss").
- Safeguarding Policy and Procedures; ETC International College Policy and Procedures for the Protection of Juniors and Adults At Risk.
- Fire Safety Procedures (documented by building, see "Fire Safety" section of ETC website, 'Staff Documents' section).

The information within the above procedures supersedes any general guidance in this document: The specific documents above should be consulted and followed in the first instance for any given incident.

2.0 Contingency Procedures

2.1 Fire:

Fire response procedures are covered in individual Fire Safety Procedures (documented by building, see "Fire Safety" section of ETC website, 'Staff Documents' section).

Fire Safety Officer and line manager should be informed of any fire, no matter how small, or serious risk of fire (near miss). Similarly any damage or malfunction of fire detection, alarm, signage or fire-fighting equipment shall be referred to Fire Warden, Fire Safety Officer and line manager.

Fire Safety Officer and any line manager becoming aware of an incident, near miss or other issue as identified above will ensure that immediate steps are taken to clean up, make safe or prevent further incident or risk. They shall then inform Director of the College so that consideration can be given to further action.

Fire Safety Officer is responsible to record and report any incident that qualifies under RIDDOR or relevant Fire Safety / Health & Safety regulations or guidelines.

2.2 Major Incident (Terrorist / Firearms / Weapons Attack and Bomb Threats):

Refer to ETC International College Procedure: Response to Major Incidents (including Terrorist / Firearms / Weapons Attack and Bomb Threats).

The Crisis Management Team will coordinate the response to any such incident.

2.3 Cyber-attack:

Where a cyber-attack may compromise any aspect of delivery.
The Crisis Management Team will coordinate the response to any such incident.
A designated staff member has been assigned (AK) to deal with cyber issues and may be co-opted onto the Crisis Management Team in the event of a major incident.

Context:

- The risks and methods of cyber attacks are constantly changing and evolving, and therefore specialist advice shall be sought in the event of an incident or suspected breach of security.
- The Department for Education has been asking centres to review National Cyber Security Centre advice following increasing number of cyber-attacks involving ransomware infections. The NCSC information supports centres in cyber security preparedness and mitigation work.
- Ransomware attacks continue and the Department is reminding centres to review the NCSC advice and to take precautions. This includes ensuring that you have backups in place for your key services and data.

Staff will be trained and updated as necessary on the risks and safe practices to be adopted for existing and emerging threats. The Board of Governors, Crisis Management Team and IT team may initiate this training.

In the event that a cyber attack prevents or disables the use of IT systems or equipment, refer to section 2.4 'Failure of IT Systems' for further guidance, and section 4.0 'National Cyber Security Centre' for further advice and information.

Exams officers (ELT & FE/HE) will work with IT and contact the relevant awarding bodies for guidance in the event that exams or related, sensitive materials are compromised. Head of FE/HE and FE/HE Exams Officer will monitor and take action required as directed by the awarding bodies.

2.4 Failure of IT Systems:

The Crisis Management Team will coordinate the response to any such incident.
A designated staff member has been assigned (AK) to deal with IT issues and may be co-opted onto the Crisis Management Team in the event of a major incident.

Critical data is backed up on the Cloud (including Microsoft OneDrive data).
ETC college network and server contents are backed up regularly and stored in a separate, fireproof & waterproof location.
Backup systems are ready to be used in the form of additional laptops and desktops.

Separate Internet connections are provided by the College to connect to the internet. Systems in a separate building to be used as a backup.

All business-critical systems are cloud-based, allowing basic functioning of the core business without the college network/server until internal systems can be restored.

College server and network equipment are housed in a separate, locked room with restricted access. Designated IT support will be contacted immediately an incident occurs, or is suspected to have occurred. This includes breach of security to the server room or other facility containing networked computers or components.

Any member of staff becoming aware of a potential security breach (physical, data, communications or via infected software) shall be reported immediately to a member of the IT team or the designated IT support member (AK).
Any equipment suspected or potentially infected will be immediately disconnected from the network/internet and reported to a member of the IT team.

Threat to ongoing online lesson delivery will be assessed immediately. In extreme cases staff may use personal connection to the internet (e.g. teaching from home) if college systems are unavailable and with the full knowledge and permission from their line manager.
It is the staff member's responsibility to ensure the protection of college data, hardware, software and integrity in the event that personal equipment or connection is used. This includes GDPR / Data Protection or other sensitive or personal data considerations, including those of the staff member themselves.

2.5 Loss of Premises:
The Crisis Management Team will coordinate the response to any such incident.

Arrangement has been made within the Student Protection Policy (section 1 "ETC is no longer able to operate"; "ETC is no longer able to deliver courses in one or more subject areas due to inaccessible premises") for alternative accommodation for lesson delivery and core business functions.

Depending on supply and demand (and how much of ETC college is unavailable for use) alternative teaching accommodation shall be hired for face to face lessons (as per summer General English arrangements, using local hotels, colleges, schools or professional training facilities).

Online lessons may alternatively be delivered by staff using personal connection to the internet (e.g. teaching from home) if college systems are unavailable and with the full knowledge and permission from their line manager.
In this event it is the staff member's responsibility to ensure the protection of college data, hardware, software and integrity in the event that personal equipment or connection is used. This includes GDPR / Data Protection or other sensitive or personal data considerations, including those of the staff member themselves.

If the above measures are insufficient to meet demand then the Student Protection Policy will be followed in terms of out-sourcing delivery of contracted obligations.

3.0 Further guidance to inform procedures and implement contingency planning

- DfE
- Ofqual
- Ofqual guidance extract taken directly from the Exam system contingency plan: England, Wales and Northern Ireland - What schools and colleges and other centres should do if exams or other assessments are seriously disrupted

- Health & Safety Executive (https://www.hse.gov.uk/), guidance (https://www.hse.gov.uk/guidance/index.htm) and reporting (https://www.hse.gov.uk/contact/tell-us-about-a-health-and-safety-issue.htm)
- Fire Safety in the Workplace (https://www.gov.uk/workplace-fire-safety-your-responsibilities)
- Emergency planning and response (www.gov.uk/guidance/emergencies-and-severe-weather-schools-and-early-years-settings) from the Department for Education in England

4.0 National Cyber Security Centre

- The NCSC's free Web Check (ncsc.gov.uk/information/web-check) and Mail Check (ncsc.gov.uk/information/mailcheck) services can help protect schools from cyber-attacks. Two NCSC cyber security services, which are already helping thousands of organisations to protect their websites and email servers from cyber-attacks, are now available to all UK schools. Both tools are available free of charge, are quick to set up, and thereafter run automatically. More information is available from the NCSC website (ncsc.gov.uk/blog-post/cyber-tools-for-uk-schools).
- Ransomware advice and guidance for your IT teams to implement (ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks)
- Offline backups in an online world (ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)
- Backing up your data (ncsc.gov.uk/collection/small-business-guide/backing-your-data)
- Practical resources to help improve your cyber security (gov.uk/section/education-skills/cyber-security-schools)
- Building Resilience: Ransomware and the risks to schools and ways to prevent it (com/watch?v=FppzWedY0ic&t=237s)

Version: 1
Approved January 2026: Principal
Next update due: January 2028