Contingency and Adverse Effects Policy

Policy no:	1.3
Version date	01-05-25
Approved by	Board of Governors
Policy Group	Governance
Version number	V3
Next review due	May 2025
External reference points	Primary Element 2: *Sustainability* in the Council of University Chairs (CUC) Higher Education Code of Governance states: 'there are effective systems of control and risk management in place'. UK National Cyber Security Centre on How to effectively detect, respond to and resolve cyber incidents https://www.ncsc.gov.uk/collection/incident-management

Version Control			
Previous Version	**New Version**	**Date**	**Update/Notes**
V1 (23-11-23)	V2	30-04-25	Added version control table. Changed the Management Director to Executive Principal as responsible for ensuring competent risk management staff are in place and that this policy is implemented. Added a new section on Cyber-attacks and cybersecurity including impacts on exams and assessments. There is also a new cyber-attack severity matrix and mitigation plans.

Contents

1. Introduction

This Contingency and Adverse Effects Policy involves identifying and preventing adverse events and ensuring that lessons are learned so they may be prevented from occurring in future. Adverse events can pose risks to Trent Education Centre (TEC) operations and this policy provides a means for ensuring that the type of adverse effects that may affect TEC are understood and there are plans in place for dealing with them and mitigating them.

2. Purpose and Scope

This policy prepares TEC for the effects of something happening that will potentially have a detrimental impact on the achievement of organisational objectives, or even in some cases on the existence of TEC. It includes risk management, which is the process of preparing for and mitigating the likelihood and potential consequences of a detrimental event occurring. Health and Safety risks are assessed and managed by TEC Health and Safety Policy. All other risks are assessed and managed by the Student Protection Plan July 2024 and a Risk Register.

TEC aims to be prepared to deal with the impact of incidents that may harm TEC, its students, staff and other stakeholders. To this end it will

- Identify a range of adverse events that can impact negatively on the College, its students and other stakeholders.
- Identify a range of critical incidents that may occur
- Ensure the development and ongoing review of risk for the College and all its activities
- Determine the method of assessing and managing risks
- Ensure staff understand their responsibilities in terms of risk ownership
- Provide an updated Contingency and Adverse Effects Plan that is fit for purpose, and aligned with the Student Protection Plan

3. Identifying Adverse Events

An adverse event may impact on TEC in the following ways:

- TEC is unable to meet its deadlines for the publication of results and handing out of certification with may impact in individual student plans and progress
- TEC fails to adequately identify academic misconduct and malpractice which impacts on the credibility of the College and the award
- Rising costs to students due to an unforeseen event e.g. moving to a new location that may prevent them from being able to complete their course
- TEC is prevented from delivering an academic programme leading to an award
- An assessment does not ensure the standards of the qualification are secure
- An assessment does not allow for a consistent distinction between the assessment of student work at different levels
- The reputation of TEC if is subjected to a criminal investigation or faces sanction from regulators or awarding organisations
- The reputation of TEC if a member of the Senior Management Team is subjected to a criminal investigation or other disciplinary proceedings
- Poor, inaccurate or misleading public information that impacts on student expectations and achievements

4. Procedure for dealing with an Adverse Event

4.1. Reporting an event or near miss

Staff must report the following to the Head of Operations if an adverse event occurs and escalate it to the Managing Director if necessary.

Your Name		**Your Contact**	
What adverse event has occurred? **Describe it briefly**		**Who are directly affected by the event?**	
Date and time of the event		**Location of the event**	
What caused it to happen?		**What action has been taken so far?**	
How severe is the event?	Low ☐	Medium ☐	High ☐

4.2. Adverse Events Team

If there is an adverse event of the kind identified in the section above, the Adverse Events Team will investigate it and make recommendations to the Senior Management Team and Board of Governors if required:

- Head of Operations
- Managing Director
- Executive Principal
- Head of Compliance
- Head of Quality
- Head of Higher Education

4.3. Notification to Pearson Awarding Organisation

It may be necessary to report some critical incidents or adverse effects to TEC's Awarding Organisations (e.g. ATHE or Pearson) if the incident or adverse effects lead to one of the following:

- TEC becomes insolvent or faces bankruptcy proceedings.
- There is any change in ownership of TEC.
- There is a significant change to the way in which the College is governed or its legal status.
- TEC should merge with any other entity.
- There has been event that adversely affects student studying for the ATHE or HND award.
- A student wishes to transfer to another centre offering the same award

The TEC Adverse Effects Team provided above will determine if there is a need to inform the awarding organization and if there is, will appoint one person to contact the awarding organization without delay and provide the following:

- How many students are affected
- How serious the event is
- If the event is due to misleading information published by TEC
- The qualifications and units affected if relevant
- How the incident was first reported
- All the parties involved and aware of the incident
- A plan of action showing what steps have already been taken and what is next

5. Identifying Risks

The risk management process, excluding risks that fall more generally under the category of Health & Safety threats and hazards, are based on an assessment of risks including those identified in the Student Protection Plan and Risk Register. Risks may be added or removed, and the Risk Register is updated every four months. The following list, which is not exhaustive, includes risks that may be identified and assessed in the Risk Register:

- Student Recruitment
- Admissions Process
- Student Engagement Progression
- Student Learning
- Resources to Enhance the Student Experience
- Key Staff Retention
- Financial Resources
- Information Resources
- External Policy Environment
- Student Voice
- Student Experience
- Marketing Strategy
- Governance
- Reputation
- IT Infrastructure and GDPR
- Growth Targets
- Closure of the College
- Closure of a Course or Courses
- Change in Course Content
- Change in Location
- Limitations due to the Pandemic or Natural Disaster
- Change in law

6. Identifying Critical Incidents

The following are examples of critical incidents that may occur. This list is not exhaustive:

- The loss of data or breach of confidentiality through cyber attack
- A student, staff member or other stakeholder dies as the result of an accident, illness or crime
- A student, staff member or other stakeholder has a serious injury
- A student, staff member or other stakeholder is physical attacked and harmed
- Collapse of TEC buildings.
- Threats to public health, such as outbreaks of meningitis or a pandemic.
- Severe weather conditions disrupting normal activities.
- Accidents involving transportation.
- Civil disturbances or acts of terrorism.

6.1. Assessing Risk – Student Protection Plan

The risks in the table below include a likelihood and an impact score of 1-5. A low score of 1 or 2 means a very low risk, and a high score of 4 or 5 is a very high risk. When the likelihood and impact score are multiplied together, the overall rate of risk can be identified as follows:

1-5	Very Low Risk	6-10	Low Risk
11-15	Medium Risk	16 – 20	High Risk
21 – 25	Very High Risk		

All risks are explained according to how well they are currently being managed of controlled. Deadlines are also provided for further mitigations that are planned to help prevent the risk from occurring and to minimise its impact if it does.

6.2. Senior Management Team

The Student Protection Plan and the overall management of risk including the review, update and implementation of this policy is the responsibility of the Senior Management Team (SMT) which carries out the following functions at its quarterly meetings:

- Overseeing the effectiveness of and adherence to established policies in relations to risk and risk management including this policy
- Revising and enhancing relevant policies and procedures to address existing risks effectively.
- Assessing the College's risk management framework to guarantee all essential risk areas are addressed.
- Identifying and suggesting new risk areas as they become necessary.
- Implementing measures to mitigate risks and reduce their potential adverse impacts.

6.3. Risk Owners

Each risk identified must have a risk owner, who is responsible for ensuring their assigned risk area is effectively monitored and mitigated. The risk register remains live and is updated by all risk owners every quarter or soon if the urgent need arises.

6.4. General Staff Responsibilities

All TEC staff members are tasked with identifying, reporting, and managing risks effectively. Specific risk ownership is delegated to staff members by the Senior Management Team. Staff are required to provide updates on risk controls and risk mitigation plans for the risks assigned to them, including the execution of strategies to reduce risks, ensuring these align with broader planning procedures and activities.

6.5. Head of Operations (HO)

The TEC Head of Operations is responsible for ensuring effective risk management processes and competent managers are consistently in place. Comprehensive risk assessment and management must be conducted to identify and mitigate risks across all TEC services, whether delivered online or on-site at any campus. Risk assessments should be integrated into the planning, development, and expansion of TEC provisions, facilities, and resources.

7. Risk Management Process

The process of risk management at TEC has the following steps:

1. The control status and implementation of all risk mitigation plans is monitored by risk owners
2. Risk owners update the control status and mitigation plans of all risks they are responsible for
3. Risk owners report on the risks they are responsible for to the Senior Management Team (SMT) every quarter.
4. The Senior Management Team discusses and approves the updated risk register together with all control updates and mitigation plans every quarter

8. Critical Incident

8.1. Aim

Whenever a critical incident occurs, there must be a critical incident management team in place ready and able to react promptly and effectively so that the any harm or damage is either prevented or minimised. An appropriate response from the (CIMT) must be in place quickly to informs all stakeholders and people at risk about the nature and extent of the incident and what steps are being taken to prevent or minimise harm or damage from occurring.

8.2. Critical Incident Management Team (CIMT)

- Managing Director
- Executive Principal
- Head of Operations
- Head of Quality
- Head of Higher Education
- Head of Compliance

Other staff, governors or stakeholders may be co-opted as members of the CIMT if needed. CIMT may also contact partners who may support and participate in any emergency planning and mitigations. The MD will lead CIMT in taking steps to deal with any critical incident. In the absence of the MD, the Executive Principal with lead the CIMT. The following scenarios provide some guidance on how critical incidents will be handled by CIMT.

9. Terrorist Incident Occurs

TEC informs all its students, staff and other stakeholders to follow the UK government's recommendations on dealing with a terrorist incident, especially if it involves someone with a weapon such as a gun or knife or any explosives. The key government recommendation involves Hiding, Running and Telling if a terrorist incident occurs anywhere including on excursions outside or in a TEC building or other facility occupied by TEC students, staff and stakeholders engaged in activities organised by or on behalf of TEC.

https://www.counterterrorism.police.uk/safetyadvice/

If a critical incident such as a terrorist attack affects TEC stakeholders during activities arranged by or for TEC stakeholders, the following steps must be taken:

- Emergency services 999 must be contacted.
- The Head of Operations must be informed.

The Head of Operations will organise the required action which will include:

- Arranging transportation if necessary to take people home or to safety
- Informing the Critical Incident Management Team (CIMT) members
- Calling a meeting of the CIMT to agree on a plan if necessary

The CIMT briefs and advises students and staff about the incident and what they need to do to stay safe.

10.Procedure for Handling Cyber Attacks

TEC follows the guidelines set out by the National Cyber Security Centre (see link below) in order to deal effectively with the detection, response and resolution of cyber incidents particularly to the extent that they may affect students.

https://www.ncsc.gov.uk/collection/incident-management

10.1. Preparation and Prevention

TEC takes the following steps to prepare for and prevent the likelihood and impact of cyber-attacks:

- Maintaining an up-to-date inventory of IT systems, networks, and software to ensure that all impacts of cyber-attacks can be identified and rectified by IT staff
- Conducting training in cybersecurity for staff and to a lesser extent for students
- Implementing robust firewall and antivirus solutions across all devices in all Study Centres
- Regularly backing up critical data to secure, off-site or virtual locations.
- Carrying out periodic vulnerability assessments and penetration testing.

10.2. Detection and Reporting

TEC proactively monitors all its IT systems for unusual activity using automated tools and manual checks. TEC also instructs all staff and students on the need to notify the TEC Cyber Incident Response Team (CIRT) as described below about any suspicious activity that may involve cyber threats and attacks, and these are investigated by CIRT. Low level incidents may be handled by the IT Manager alone. However, higher level incidents that may compromise service delivery or confidential data must be escalated to the CIRT.

10.3. Critical Incident Response Team

The Cyber Incident Response Team (CIRT) includes the following TEC members:

- IT Manager
- Finance Manager
- Managing Director
- Executive Principal
- Head of Operations
- Head of Compliance

10.4. Critical Incident Response

The CIRT is activated as soon as there is a threat or actual cyber-attack that has be escalated by the IT Manager or other IT staff and the following steps are taken:

- The incident is triaged in order to understand how the specific details of the incident including its type and severity
- The cyber breach is contained by isolating affected systems or networks.
- The incident is communicated to key stakeholders, including management, staff, and students.
- Relevant authorities or regulators are notified (e.g., the Information Commissioner's Office) if personal data is involved.

10.5. Cyber-attach Severity

The severity of a cyber-attack is determined according to the following three criteria:

- **Availability** of data or systems following the attach and how this affects TEC services to students and the support it provides to staff
- **Confidentiality** of sensitive data and whether it has been stolen or leaked
- **Integrity** of any data or systems that may have tampered with so they can no longer be relied upon

Severity Level	Description	Examples	Impact
Critical	Cyber-attacks causing severe disruption to essential operations, major data breaches, or compromising sensitive information.	Attack on student/staff personal data (e.g., identity theft). Breach of exam or assessment results or academic records. Complete system failure affecting teaching and learning platforms.	Students unable to take their exams or assessments or get their result in timely fashion. Most staff unable to work effectively. No access to systems, platforms or email accounts for course delivery. Legal and regulatory consequences. Loss of stakeholder trust. Loss of partnerships. Major reputational damage. Significant financial impact.
High (Less Critical)	Attacks disrupting operations but manageable with immediate action, targeting fewer sensitive systems or data.	Ransomware affecting administrative systems- Denial-of-service attack (partial, recoverable). Malware in library access platforms.	Up to 50% of students and staff are affected through loss of data and lack of access to systems or email accounts. Some examinations or assessments may be compromised. Temporary disruption to operations. Potential reputational harm. Costly recovery measures
Medium	Minor cyber incidents with minimal disruption, affecting non-essential services or isolated issues.	Phishing attempt targeting a few staff or students. Malware infecting individual devices. Low-scale unauthorised access.	Limited operational impact. Minimal reputational concern Quick resolution possible with minimal resources.

10.6. Mitigations if a Critical-Level Cyber-Attack Occurs

When dealing with a critical-level cyber-attack, TEC will seek consultation with Spectrum Technical Services https://spectrumtechnical.co.uk/ which uses Ubiquiti software https://www.ui.com/ for the provision of TEC's firewall.

- Immediately activate the Critical Incident Response Team (CIRT).
- Isolate affected systems to prevent further damage.
- Neutralize the threat by addressing vulnerabilities and removing malware or compromised accounts.
- Restore systems and data from backups, ensuring integrity checks are completed.
- Notify regulatory bodies (e.g., ICO) and all stakeholders promptly.
- Engage cybersecurity experts for containment and resolution.
- Enhance security post-incident with updated protocols and employee training.
- Keep detailed records of all recovery actions taken.
- Support affected individuals, including offering guidance on protecting their accounts and data.
- See below for further guidance on mitigation measures for cyber-attacks affecting exams and assessments

10.7. Mitigations if a High-Level Cyber-Attack Occurs

- Escalate the issue to the IT Manager for immediate action.
- Isolate and restore affected systems from backups.
- Communicate with staff and students to manage disruptions.
- Identify vulnerabilities and address them with updated software patches.
- Keep detailed records of all recovery actions taken.
- Support affected individuals, including offering guidance on protecting their accounts and data.
- See below for further guidance on mitigation measures for cyber-attacks affecting exams and assessments

10.8. Mitigations if a Medium-Level Cyber-Attack Occurs

- Resolve the issue at the Programme Leadership level.
- Provide affected staff or students with support and guidance.
- Monitor for any signs of escalation.
- Review and adjust user access controls if necessary.

10.9. Cyber Attacks during Exams and Assessments

Dealing with a cyber-attack during exams and assessments requires a clear, focused approach to ensure minimal disruption and preserve the integrity of the examination or assessment process. In the event of an attack, the first priority must be the immediate containment of the incident to secure all digital systems related to exams and assessments. Communication with students and staff is vital; they should be informed promptly of any disruptions and provided with instructions on how to proceed. Alternative arrangements may need to be implemented, such as shifting to offline or manual examination methods if systems cannot be restored quickly. Additionally, a review of affected systems should be conducted to assess whether any exam or assessment data has been compromised, and necessary steps must be taken to recover or safeguard this information. TEC must coordinate with relevant bodies, such as examining boards or regulatory authorities, to ensure compliance and transparency throughout the process. Once the situation has been resolved, steps should be taken to enhance security measures to prevent future occurrences during critical periods like exams.

10.10. Post-Incident Review

After a cyber-attack TEC will conduct a thorough review that includes the following:

- Conduct a thorough analysis of the attack, identifying weaknesses and lessons learned.
- Update security measures and protocols based on findings.
- Provide a report to the Senior Management Team (SMT) on the incident and improvements made.
- Schedule follow-up assessments to ensure ongoing protection.

11.Communication in a General Emergency Situation

- A designated member of the Critical Incident Management Team (CIMT) will handle communication with emergency services using a mobile phone.
- A designated member of CIMT will communicate with media outlets on behalf of TEC if required.
- TEC's primary contact line, **+44 (0)7368971605**, will serve as the point of contact for incoming calls.
- TEC may use an emergency 24-hour mobile phone number if needed.
- Mobile phones will be used for all outgoing calls during the incident.
- Staff managing incoming calls must maintain records of the date, time, caller details, and the content of the conversation.
- All calls will be recorded if possible.
- A person nominated by the Critical Incident Management Team will handle all media enquiries and no-one else will communication to the media including responding to emails or phones calls without approval by the Critical Incident Management Team.

12.Where to go in an Emergency

In an emergency, CIMT and any other stakeholder needing help, support or information should go to the **Control Centre** at TEC's Head Office: Digital House 2.3, Clarendon Park, Nottingham, NG5 1AH. If TEC's Head Office is unsafe for any reason, TEC CIMT will inform all stakeholders of an alternative location for the Control Centre during and immediately after a critical incident.