Reviewer: Executive Team
Version: 11
Review Date: 01/11/2025
Next reviewed: 01/11/2026
Document Number: GOV-002-R9

Business Continuity and Disaster Recovery Plan

Applicability

This policy applies to all divisions, subsidiaries, departments, and associated Twin organisations, including Twin Education Centre Ireland (TECI) and any other delivery locations.

It is binding on all employees, contractors, subcontractors, delivery partners, and stakeholders who undertake activities on behalf of Twin, regardless of business unit, delivery model, or geographical location.

Where services are delivered through subcontracted or partnership arrangements, those organisations are expected to operate in line with the principles of this Business Continuity and Disaster Recovery Plan (BCDRP) and to maintain appropriate continuity arrangements that align with Twin requirements.

All parties engaged in delivering services on behalf of Twin are expected to adhere to the principles, standards, and requirements set out in this document.

Introduction

This BCDRP sets out the procedures and guidance required to ensure the continued operation and recovery of services in the event of a disruption or disaster affecting Twin operations. This includes incidents that result in the loss of, or restricted access to, Twin Headquarters in Greenwich, other UK operational sites, the Dublin English Centre (TECI), and remote working locations.

The plan also applies to services delivered through subcontracted provision, delivery partners, and third-party suppliers where these form part of Twin's contracted delivery responsibilities.

The plan also addresses a range of potential business continuity risks that could affect service delivery across all Twin locations, including:

- IT security breaches or cyber incidents
- Loss or failure of a major supplier or sub-contractor
- Widespread illness or staff shortages
- Transport disruption
- Severe weather events
- Building or infrastructure failures
- Other operational disruptions affecting the delivery of services to customers and learners

Implementing an effective recovery plan as quickly as possible following a disruption provides significant benefits, including:

- Rapid restoration of operational capability
- Minimisation of financial and operational loss
- Maintenance of service levels to meet contractual and regulatory obligations
- Preservation of relationships with suppliers, partners, and stakeholders
- Ensuring that customers and learners, continue to receive services in a safe and professional manner

The safety and wellbeing of staff, students, customers, and visitors and learners participating in programmes delivered through subcontracted or partnership arrangements is the highest priority in any incident. The plan therefore identifies several key actions designed to ensure a prompt and coordinated response and to limit the impact of any disruption as far as reasonably possible. These include:

- Providing immediate assistance in the event of casualties and ensuring appropriate welfare support, including counselling for staff, students, or customers if required
- Communicating promptly with staff, students, customers, subcontracted delivery partners where relevant, and stakeholders to provide updates on the situation and outline recovery plans
- Relocating staff and operational activities from affected premises to an appropriate recovery site where necessary
- Ensuring that all critical IT, communication, and operational systems are restored and functioning as quickly as possible

This plan applies to all operations. Where site-specific considerations apply, such as student communications, classroom relocation, or temporary transition to online learning, these are addressed within the relevant sections of this document. Where services are delivered through subcontractors or delivery partners, Twin will work with those organisations to ensure continuity arrangements align with the principles of this plan.

It is recognised that it is not possible to anticipate every potential scenario. The guidance contained in this plan therefore provides a structured framework for response and recovery, while allowing flexibility depending on the nature, scale, and severity of the incident. In the event of a major disruption, the Incident Management Team (IMT), led by the Managing Director – International, who will coordinate the response in consultation with emergency services and relevant authorities.

The BCDRP will be reviewed and updated regularly by the Chief People Officer to ensure it remains accurate and effective. Updated versions will be distributed to relevant personnel accordingly. The Head / Director of each business unit is responsible for maintaining and updating their own departmental continuity procedures and for communicating any changes to the Chief People Officer.

Where services are delivered through subcontracted arrangements, the relevant contract manager must ensure that subcontractors maintain appropriate business continuity arrangements and that these align with Twin's requirements.

Further guidance on document maintenance and review processes is provided later in this document.

All individuals referenced within this plan are responsible for notifying Human Resources of any changes to their personal contact details and informing the Chief People Officer of any changes to operational procedures or areas of responsibility as soon as they occur.

This plan contains the information required to recover from a total loss of, or denial of access to, Twin's primary office at:

The Greenwich Centre
12 Lambarde Square
London
SE10 9GB

As well as other Twin operational locations, including satellite centres and the Twin English Centre Ireland (TECI) in Dublin at:
4 North Great Georges Street
Dublin 1
Republic of Ireland.

Other Continuity Scenarios

In some situations, business continuity issues may arise that do not prevent Twin from operating from its premises but may still disrupt normal operations. Examples include staff shortages, localised operational disruptions, or temporary system failures, or disruption affecting subcontracted delivery partners.

In such circumstances:

- Each Head / Director of each business unit (HoBU) is responsible for informing their team members and their line manager of the issue and implementing appropriate contingency arrangements to maintain service delivery.
- In the absence of the HoBU, their designated deputy will assume this responsibility.
- HoBUs must ensure that adequate backup plans are in place to maintain operational continuity until the issue is resolved.
- Where disruption affects subcontracted provision, the relevant contract manager must liaise with the subcontractor to ensure appropriate contingency arrangements are implemented and that learners continue to receive support.
- If an entire department becomes unavailable, responsibility for continuity planning transfers to the HoBU's line manager, who must ensure that appropriate arrangements are implemented.

These operational continuity arrangements will be reviewed regularly as part of monthly operations meetings, during which capacity planning, staffing levels, and system performance are assessed. Any required adjustments will be implemented to ensure the continued resilience and effectiveness of Twin's operations across all locations, including the Dublin English Centre (TECI).

1. Purpose

The purpose of this policy is to:

- Ensure the safety of staff, students, customers, and stakeholders.
- Protect and maintain Twin's critical business functions across all operational locations, including services delivered directly or through subcontracted and partnership arrangements.
- Safeguard data, IT systems, and operational infrastructure.
- Provide clear guidance for emergency response, recovery, and communication during incidents that may disrupt operations across Twin sites or services delivered on its behalf.

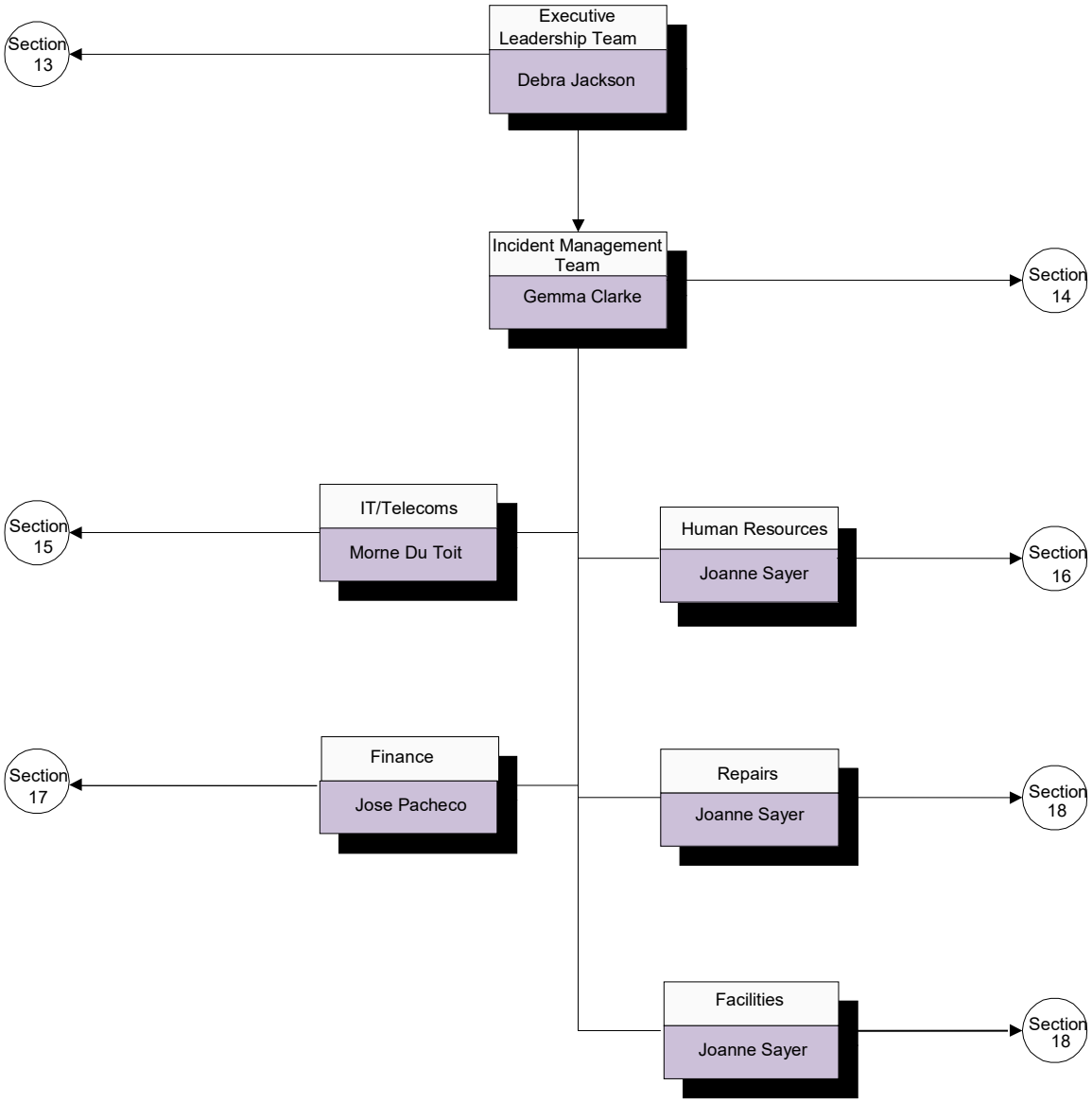
2. Scope

This policy applies to:

- All Twin employees and contractors and subcontractors delivering services on behalf of the organisation at every site, including the Dublin Centre.
- All IT systems, software, and data, including Prime Systems and remote desktop infrastructure.
- All critical business processes and educational delivery functions, including those delivered through subcontracted or partnership arrangements.
- Emergency response, recovery, and communication with internal and external stakeholders.
- Subcontracted delivery partners are expected to maintain appropriate BCDRP arrangements that align with the principles of this policy and support the continued delivery of services to Twin learners and customers.

Contents

3. Governance & Responsibilities



3.1 Senior Leadership Team (SLT) Governance

- Reviews and confirms business continuity and disaster recovery arrangements.
- Confirms recovery strategy and oversees execution across all sites.
- Receives updates on critical incidents and directs coordination for financial and logistical support.
- Authorises media statements during incidents.

Frequency of Review: Annually or upon milestone/critical incident.

3.2 Incident Management Team (IMT)

- Ensures standby services are adequate and operational.
- Coordinates plan updates and testing with Recovery Team Leaders.
- Conducts **user tests annually** or "walk-throughs" if full testing is not possible.
- Ensures insurance and critical service backup plans are in place.

Frequency of Review: Every six months; annual full review.

3.3 IT Team

- Maintains software, data, and hardware recovery procedures.
- Ensures offsite backups are current and verified.
- Maintains contact with suppliers for rapid replacement of critical equipment.
- Conducts penetration tests and periodic restore drills, including involvement of non-key staff.
- Maintains telephony and standby centre documentation.
- Supports all sites, ensuring remote desktop infrastructure enables continuity.

Frequency of Review: Every six months or upon significant system change.

3.4 Business Functions

- Confirms critical activities and necessary standby resources.
- Develops emergency accounting and expenditure procedures.
- Maintains site-specific emergency manual procedures.
- Ensures classrooms and student delivery continuity are included in all plans.

3.5 Centre Staff Responsibilities

- Recognise hazards (fire, electricity, chemical, social, crushing).
- Report hazards to Centre Manager or escalation line:
    1. Operations Manager
    2. Director / Director of Studies
    3. Head of Operations / site senior staff
    4. SLT (Emergency Team)

- At the Dublin Centre, Centre Manager ensures immediate coordination with SLT and communicates operational instructions for TECI students.

4. Emergency Response Controller (ERC)

- Takes ownership of incident once management identifies the lead.
- Responsibilities:
    1. Ensure staff, student, and stakeholder safety.
    2. Execute relocation to the nominated second site or safe exit.

3. Safeguard customer/student data via relevant authorities.
4. Contact Immediately Required People list.

- **Dublin Centre Specific:** ERC coordinates rapid contact to all TECI students; advises alternative venues or online delivery if classrooms unavailable.

5. Recovery Locations

Site	Primary Recovery	Secondary Recovery	Notes
Southwark site: 224-236 Walworth Road Manor House, SE17	Greenwich HQ site: 1st Floor, The Greenwich Centre, 12 Lambarde Square, Greenwich, London, SE10 9GB	N/A	Ensure customer contact, data continuity, minimal exposure of hard copy data
Dublin (TECI) Site: 4 North Great George's Street, Dublin 1	Ad hoc classroom rental space is available	N/A	Classes may move online until site restored; student communications critical
Greenwich HQ site: 1st Floor, The Greenwich Centre, 12 Lambarde Square, Greenwich, London, SE10 9GB	Southwark site: 224-236 Walworth Road Manor House, SE17	N/A	Finance/Admin recovery
Eastbourne site: Compton Park, Compton Place Road, Eastbourne, BN21 1EH	Ad hoc classroom rental space is available	N/A	Classes may move online until site restored;
Leicester site: 2nd Floor, 60 Charles Street, Leicester, LE1 1FB	Ad hoc classroom rental space is available	N/A	Classes may move online until site restored;

6. Staff Contact & Remote Working

- Staff with PCs at home can work remotely during incidents.
- **Dublin Centre Staff Remote Access:** TECI staff must ensure remote desktop and broadband are functional; Prime Systems accessible.

7. Risks

Risk	Impact	Management Approach	Contingency
Users cannot access data	Medium	Routine maintenance, backups, UPS power	Switch on backup servers, replace PCs, quarantine, notify relevant personnel
Backup failure	Low	Verified secure backup schedule (on-site/off-site/shadow copies)	Restore from alternate backup
Unauthorised data access	Medium	Encryption, access control, monitoring	Notify authorities, restore data, assess policies
Accidental deletion	High	Three types of backups	Restore from backup, retrain users
Email virus/phishing	High	Antivirus, user awareness, patching	Quarantine machines, freeze outgoing emails, clean up
Web browser threats	High	Awareness, antivirus, firewall policies	Quarantine affected devices, clean up
External hacking	High	Firewall logs, alerts	Notify authorities, disconnect sessions, restart firewall
Physical security breach	Medium	Alarms, secure rooms, restricted access	Notify authorities, rebuild systems from backup
Loss of subcontractor	Medium	SLAs, performance management	Redirect services to other partners

7.1 Dublin Centre Considerations

- No electronic data stored locally; remote desktops handle all delivery.
- Hard copy data minimal, locked in line with Security Policy.
- Students may continue online until physical site restored.

8. Testing & Maintenance

- **IT Recovery Test at Recovery Site:** Every 6 months (last Feb 2025)
- **Tabletop Test with Recovery Teams:** Every 6 months (last Feb 2025)
- **Full IT & Recovery Simulation:** Yearly (last Feb 2025)
- Updates to BCDRP communicated to all affected teams.
- Minimum update frequency: **annually or upon critical incident**.

9. Media & Communication

- Only SLT-approved personnel issue statements.
- Statements emphasise cooperation, safety, and operational recovery.
- Avoid commenting on: casualties, cost estimates, damage extent, or responsibility.
- Student and parent communications via email or website; online learning updates if classrooms unavailable.

10. Document owner / distribution

10.1 Document owner

This document is owned by, and the Master Copy held by Joanne Sayer, Chief People Officer

10.2 Distribution list

The following people have received a copy of the BCDRP:

Copy	Name	Job Title/Department	Signed	Date
	Joe Sayer	Chief People Officer		
	Caroline Fox	Chief Executive Officer		
	Jacqui Fox	Director, Strategic Partnerships		
	Jose Pacheco	Financial Controller		
	Morné Du Toit	Director of IT		
	Debra Jackson	Divisional Managing Director, International		
	Gemma Clarke	Academic Director		
	Lynsey Whitehead	Assistant Director, Education & Skills		
	Keshia Siniara	Group Head of Marketing		

10.3 Amendments in this version

Date	Description	Author
15/07/2025	General review and updated people structure	Sharon Major
01/02/2026	General review	Lynsey Whitehead

10.4 Redactions in this version

Date	Description	Author

11. Layout of the BCDRP

The BCDRP provides a detailed overview of the recovery arrangements and operational procedures that will be followed in the event of a disruption to Twin services. It provides guidance to the various teams and business units who may be involved in responding to and recovering from an incident across all Twin operational locations, including the Twin English Centre Ireland (TECI) in Dublin and any services delivered through subcontracted or partnership arrangements.

The plan outlines the responsibilities of the following roles and teams:

- the Emergency Response Controller (ERC): responsible for initial response actions and first call-out procedures
- the Senior Leadership Team (SLT): responsible for strategic decision making, oversight, and communications with key stakeholders
- the Incident Management Team (IMT): responsible for coordinating the recovery response, damage assessment, salvage arrangements, and liaison with insurers and relevant authorities
- the Infrastructure Recovery Team: responsible for setting up and maintaining recovery sites, restoring IT systems, and ensuring communications infrastructure is operational
- the business units: responsible for the continuation of critical business processes and service delivery, prioritised according to time criticality agreed with each business unit
- contract managers and operational leads responsible for subcontracted provision: responsible for liaising with subcontracted delivery partners to ensure continuity arrangements are implemented and that learners continue to receive appropriate support

The following supporting plans and operational documents are hosted on the company intranet:

- Business Plan
- IT Security Plan
- HR Procedures
- Company Policies and Guidelines
- Staff Contact Details
- Premises Details

11.1 Recovery Strategy

If the Twin Headquarters in Greenwich, the Twin English Centre Ireland (TECI) in Dublin, or any other Twin delivery site becomes unavailable due to an incident or disruption, the BCDRP will be invoked.

Staff and customer transport arrangements will be prepared to relocate operations to a defined recovery site within the relevant delivery locality where appropriate. Where relocation is not immediately possible, staff may be instructed to work remotely and customers, learners, and stakeholders will be advised not to attend the affected premises.

Where services are delivered through subcontracted provision, the relevant Twin contract manager will liaise with the subcontracted organisation to confirm their continuity arrangements and ensure that appropriate contingency measures are implemented to maintain learner support and programme delivery wherever possible.

Where appropriate, delivery may temporarily transition to remote or online formats until normal operations can be safely resumed.

For sites outside of the London area, including the Dublin English Centre (TECI), staff are to work from home where possible pending further instruction from their Business Unit Manager, Centre Manager, or the nominated local Emergency Response Lead.

Learners, students, and participants will be safely dismissed from the affected premises with immediate effect where required, and parents, guardians, employers, or referring organisations (where applicable) will be notified in accordance with safeguarding and communication procedures.

Where learners are participating in programmes delivered through subcontracted partners, Twin will work with the delivery partner to ensure appropriate communication is issued to learners and that continuity of learning and support is maintained wherever reasonably possible.

12. Emergency response controller

The Emergency Response Controller (ERC) is the individual responsible for providing the initial on-site response to a serious incident or emergency affecting Twin premises, operations, or activities.

This role applies to all Twin operational sites, including the Twin English Centre Ireland (TECI) in Dublin, satellite centres, and any locations where services are delivered on behalf of Twin.

12.1 Responsibilities of the ERC

The Emergency Response Controller (ERC) is responsible for coordinating the initial response to any emergency incident affecting Twin premises, staff, learners, or visitors. This role applies to all Twin sites, including and any satellite or partner locations.

During office hours, the Emergency Response Controller will normally be the first authorised individual to attend and assess the situation. They will retain responsibility for coordinating the initial response until the premises have been safely evacuated and the severity of the incident has been determined. Control will then transfer to the most senior member of the Senior Leadership Team (SLT) present or designated Incident Management Team lead.

Outside of office hours, a designated keyholder or authorised site representative will assume responsibility for the initial response until the most senior available member of the SLT has been alerted and assumed responsibility.

At Dublin or other satellite sites, local staff act as the initial responders. They will:

- Follow local emergency procedures.
- Notify the ERC immediately.
- Evacuate staff, learners, and visitors to designated safe assembly areas.
- Provide an initial assessment of the incident.

The ERC will then:

- Take over coordination and provide leadership remotely or on site if necessary.
- Liaise with emergency services and building management as required.
- Determine whether the Incident Management Team (IMT) should be convened.
- Ensure follow-up actions, communication, and incident reporting are completed.

At locations operated by delivery partners or subcontractors, the relevant site manager or designated responsible person will undertake the initial response in line with their local emergency procedures and will immediately notify Twin through the appropriate contract manager or operational lead.

The key roles and responsibilities of the Emergency Response Controller include:

- Providing instructions to the required emergency services where necessary
- Identifying danger areas that must be avoided
- Identifying safe assembly areas

- Ensuring that the building or affected area is safely evacuated
- Conducting an initial assessment to establish the severity and nature of the incident
- Determining the immediate course of action (including escalation to the SLT.
- Convening the Incident Management Team where the situation is serious
- Notifying and liaising with emergency services and building management where applicable
- Initiating evacuation procedures and ensuring staff, learners, and visitors are accounted for

Where an incident affects subcontracted delivery sites or partner locations, the relevant Twin contract manager must be notified immediately to ensure appropriate oversight, communication, and support arrangements are implemented.

Once the Incident Management Team has been convened, the role of the Emergency Response Controller ceases and responsibility for managing the incident transfers to the Incident Management Team and Senior Leadership Team.

Responsibility for ongoing liaison with emergency services may transfer to facilities management, building management, or other designated site personnel, depending on the location and circumstances of the incident.

The emergency response controller will be one of the following people:

Name	Title/Role	Location	Contact Details
Morné Du Toit	Chief Fire Warden / Key holder / Director of IT	Greenwich	07772003045
Joanne Sayer	Chief People Officer (also responsible for Facilities)	Greenwich	07969 010586

In the event of emergency at a satellite location, please contact Joanne Sayer (07854 250911) to coordinate the response. Where Joanne Sayer is not available, please contact Gemma Clarke (+353 857593956).

12.2 ERC's requirements

The emergency response controller will need floor plans, access to a telephone and a telephone list of Incident Management Team contacts.

These are retained by the Facilities Management.

12.3 Keyholders Instructions for Access to HQ Main office

Authorised keyholders are issued with three keys that provide access to the main entrances of the Twin Headquarters office.

When the Building Manager leaves the premises at approximately 8:00 pm, the reception entrance and rear entrance doors will be locked. Access outside normal operating hours can only be gained by authorised keyholders using the issued keys.

Intruder Alarm System

The intruder alarm system is activated each weekday evening and monitors:

- All floor areas
- Access doors
- Stairwells

The alarm control panel is located in the reception area.

Deactivating the Alarm

To deactivate the alarm when entering the building:

- Enter the building through the front entrance using your key.
- Go directly to the alarm control panel located in reception.
- Enter your four-digit security code to deactivate the system.

Activating the Alarm

To activate the alarm when leaving the building:

- Ensure that all staff have left the premises.
- Confirm that all rooms have been vacated and internal areas secured.
- Ensure all doors are closed and the rear door is locked.
- Enter your four-digit security code on the alarm control panel.
- Press the “Yes” button to activate the alarm system.
- Exit the building immediately via the front door.

12.4 Dublin Site – Twin English Centre Ireland (TECI)

The Twin English Centre Ireland (TECI) in Dublin operates its own building access and security procedures in accordance with local building management requirements.
Authorised personnel at the Dublin site will be issued with appropriate building access credentials or keys as determined by the Centre Manager and building management.

Security procedures at the Dublin site include:

- Controlled building access for authorised staff
- Local alarm and building security systems
- Building management oversight where applicable

Staff must follow the site-specific access and alarm procedures issued by the TECI Centre Manager.

These procedures include guidance on:

- Access to the building outside normal operating hours
- Alarm activation and deactivation
- Building security checks when opening or closing the premises

Any security issues, alarm activations, or access concerns at the Dublin site must be reported immediately to the TECI Centre Manager and the Twin Senior Leadership Team where appropriate.

12.5 Satellite Centres

Satellite centres operate equivalent access and security procedures.

Local site managers are responsible for ensuring that keyholders and authorised personnel are familiar with the relevant building access and alarm arrangements for their location.

13. Senior Leadership Team

13.1 Senior Leadership Plan

The Senior Leadership Team (SLT) is responsible for the strategic oversight and decision-making required to manage significant incidents affecting Twin operations.

The SLT normally meets to review organisational performance and ensure that services are delivered in line with quality standards and contractual requirements. As part of this oversight, the SLT monitors risks that may impact operational continuity across all Twin activities, including services delivered directly, through the Twin English Centre Ireland (TECI), or through subcontracted and partnership arrangements.

Although this BCDRP considers worst-case scenarios, the SLT recognises that additional operational risks may arise that could affect service delivery. Any risks identified are reviewed and addressed through the monthly review processes, where capacity planning, operational performance, and risk management are evaluated to ensure continuity and recovery of services where required.

13.2 SLT Responsibilities

The SLT is responsible for managing the strategic response to a major incident or disruption affecting Twin operations. This includes overseeing the continuity of service delivery, supporting operational teams, and providing direction to the Incident Management Team where necessary.

Key responsibilities include:

- Managing the strategic response to the incident and overseeing organisational recovery
- Providing leadership and direction to the Incident Management Team (IMT)
- Ensuring appropriate communication with Commissioners, regulators, partners, and key stakeholders
- Taking overall responsibility for staff and learner welfare
- Maintaining relationships with partners, subcontractors, and suppliers to support continuity of service delivery
- Authorising significant or unforeseen expenditure required to manage the incident
- Ensuring the Board is informed and updated on the situation
- Authorising decisions relating to site recovery, refurbishment, relocation, or alternative delivery arrangements

Where services are delivered through subcontracted or partner organisations, the SLT will ensure that appropriate oversight is maintained and that delivery partners implement suitable continuity arrangements to minimise disruption to learners and customers.

Recovery Objectives Assuming High Risk	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks.	>4 wks.
Manage strategic response and communication to Commissioner	1 Day	0	0	0	0

Liaise closely with business teams via regular meetings	1 day and ongoing regular meetings	0	0	0	0
Meet regularly with Incident Management Team	1 day and ongoing regular meetings	0	0	0	0
Take overall responsibility for staff welfare	1 Day	0	0	0	0
Manage business relationships to ensure effective continuation of service delivery	1 Day	0	0	0	0
Authorise expenditure of large unforeseen amounts (depending on authority levels)	1 Day	0	0	0	0
Ensure Board are aware of situation	1 Day	0	0	0	0
Authorise decision to refurbish primary site or seek new premises	2 - 3 Days	0	0	0	0

13.3 SLT Location

Where relocation from the Greenwich HQ is required following a major incident, the SLT recovery site will normally be based at the Southwark Centre.

At the time of the incident, an authorised member of the SLT will confirm whether this location should be used as the temporary command centre.

Where the incident affects other operational sites, including the Dublin English Centre (TECI), the SLT may designate an alternative command location or operate remotely depending on the nature of the disruption.

Authorisation for relocation may be provided by:

- Members of the Senior Leadership Team
- Business Owners
- The TECI Centre Manager (for incidents affecting the Dublin site)
- Other designated senior leaders as outlined in the Emergency Response Controller list.

13.4 SLT Vital records

The Senior Leadership Team's Recovery SharePoint site is maintained through the Twin portal and is securely protected.

In the event of a cyber incident, loss of IT services, or software failure, a secure paper copy of essential recovery documentation will be retained at:

Twin Headquarters – Greenwich
12 Lambarde Square
London SE10 9GB

Southwark Centre
224–236 Walworth Road

4th Floor, Manor House
London SE17 1JE

Equivalent operational documentation is also maintained for the Dublin English Centre (TECI) to support local continuity arrangements where required.

13.5 SLT Recovery SharePoint Site contents:

Recovery item	Status
Personnel listing (addresses & phone numbers)	Up to date
Key contact details (external organisations)	Up to date
Copy of Business Continuity and Disaster Recovery Plan	Up to date
Annual report stakeholders' distribution list	Up to date

13.6 SLT infrastructure needs

Item	Quantity/Timeframes				
	1 day	3 days	5 days	2 wks.	>4 wks.
Desks	2	2	2	2	2

Where the SLT operates remotely or from alternative sites, equivalent access to IT systems and communications infrastructure will be maintained through secure remote access system.

13.7 SLT Action Plan

Day 1 - Actions	Status
Agree location of Command Centre with other members	
Review business priorities and confirm recovery strategies. Inform Insurers as required.	
Make CEO aware of situation	
Hold a meeting with the IMT to understand the severity and nature of damage/attack/reputational risk, and address any immediate staff issues (i.e. injuries, shock, welfare, mental health). Agree timings of next meetings	
If necessary, authorise IMT to engage external stress counsellors for staff as required	
Hold a meeting with operational managers to understand the expected performance financial, regulatory and reputational impacts of the incident on the business. Set times and dates of next meetings.	
Retrieve Recovery SharePoint Site	
The SLT may at this stage be required to authorise any large unforeseen items of expenditure.	
Nominate a media spokesman	
Release prepared statement for internal staff to reassure them of contingency operations in place	
Release prepared statement for internal staff about how they should communicate the incident externally	
Ensure that recorded voice message on phone lines is appropriate for situation	
Agree existence of contingency arrangements to all stakeholders and third parties to all stakeholders and third parties	

1ys 2-3 – Actions and updates from day 1	Status
Hold a meeting with IMT for an update on damage assessment of primary site, IT/infrastructure status of recovery site and welfare of staff	
Devise and release a detailed statement for internal and trusted third party use.	
Brief Managers on message to be delivered to key business partners	
Communicate with commissioners, partners, subcontractors, and key stakeholders	
Update CEO and make remaining Board members aware	
Provide updates to the Board regarding the incident and recovery progress	

Days 4-5 – Actions	Status
Continue regular meetings with operational managers and directors	
Monitor recovery progress and operational performance	
Ensure senior leadership presence remains visible and accessible to staff	

Days 5-14 – Actions	Status
Continue regular coordination meetings with the Incident Management Team and operational managers	
Evaluate organisational impact and recovery progress	
Provide updates to the Board, Commissioners, partners, and stakeholders	

Days 14-28 – Actions	Status
If the primary site cannot be restored within one month, meet with the Infrastructure Recovery Team to plan longer-term recovery options	
Review the suitability of alternative sites or delivery models	
Continue liaison with the Board, Commissioners, subcontracted partners, and stakeholders	
Work with operational teams to develop a long-term recovery and service restoration strategy	

14. Incident Management Team

14.1 Incident Management Team Plan

The Incident Management Team (IMT) is responsible for the operational coordination, assessment, and implementation of recovery actions in response to major incidents affecting Twin operations. This includes services delivered directly, via the Twin English Centre Ireland (TECI), or through subcontracted and partner organisations.

All essential staff roles are identified within the IMT, and cross-training ensures continuity in the absence of key personnel. Existing continuity and response processes maintained by subcontractors or delivery partners are integrated to ensure consistent operational resilience across all sites.

In the event of an IT security breach, employees must contact their manager and the Director of IT (Morné Du Toit). The response policy is:

- Office hours: 2-hour response
- Outside office hours: 6-hour response

The IT Administrator monitors servers and firewalls continuously to detect suspicious activity. The Director of IT holds overall responsibility for resolution. Further guidance and escalation procedures are detailed in the IT Security Plan on the company intranet.

14.2 IMT Responsibilities

The IMT manages and coordinates all activities associated with the invocation of the BCDRP, ensuring staff, learners, and subcontracted delivery partners remain safe and operational continuity is maintained.

Key responsibilities include:

- Managing the strategic operational response to incidents at any Twin site, including TECI and subcontracted sites
- Coordinating evacuation of buildings, staff, learners, and visitors where required
- Establishing temporary coordination points near affected sites
- Liaising with emergency services and authorities
- Communicating recovery plans to the SLT, business units, and relevant delivery partners
- Securing premises and sensitive equipment
- Managing insurance claims and reporting
- Leading damage assessment, salvage operations, and overseeing health and safety compliance during recovery activities
- Overseeing repair, rebuild, or sourcing of new premises, as required

IMT recovery objectives	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks.	>4 wks.
Manage evacuation of building as required, if during working hours	1	0	0	0	0
Establish a temporary co-ordination point for staff and all visitors/participants near a damaged site.	1	0	0	0	0
Liaise with emergency services as required	1	0	0	0	0
Communicate recovery plans with SLT and business units	1	0	0	0	0
Secure damaged premises	1	0	0	0	0
Build and restore onsite systems that are not cloud hosted	0	3	0	0	0
Manage insurance claim	0	3	0	0	0
Manage damage assessment and salvage operations	0	3	0	0	0
Ensure all staff taking part in any salvage operation are briefed on any H&S matters	0	3	0	0	0
Ensure that H&S regulations are not contravened at any stage of a crisis	1	0	0	0	0
Repair, rebuild or source new premises	0	0	5	0	0

14.3 IMT Location

The IMT recovery site will be selected based on the affected location and may include:

- Twin Headquarters, Greenwich – 12 Lambarde Square, London SE10 9GB
- Southwark Centre – 224–236 Walworth Road, 4th Floor, Manor House, London SE17 1JE
- Local offices or TECI, Dublin – 4 North Great Georges Street, Dublin 1, Ireland
- Remote/home working where physical premises are inaccessible

At the time of an incident, the IMT member on site will confirm the operational recovery location.

14.4 IMT Team Members

Name	Department / Title	Function	Contact details
Debra Jackson	Managing Director – International	Leader	07591824593
Joanne Sayer	Chief People Officer (also responsible for Facilities)	Leader	020 8269 5680
Gemma Clarke	Academic Director	Team Member	+353 857593956
Lynsey Whitehead	Assistant Director, Education & Skills	Team Member	07518906985
Jose Pacheco	Financial Controller	Team Member	07535058287
Morné Du Toit	Director of IT	Team Member	020 8269 5750
Jacqui Fox	Founder	Team Member	020 8269 5693

Note: For incidents affecting TECI or subcontracted delivery partners, the TECI Centre Manager and key subcontractor leads will be included in IMT communications and recovery coordination.

14.5 IMT Vital Records

The IMT maintains essential recovery documentation via:

- Recovery SharePoint (cloud-hosted)
- Secure paper copies at:
    - Twin Headquarters, Greenwich SE10 9GB
    - Southwark Centre, London SE17 1JE
    - TECI, Dublin 1, Ireland (supporting local continuity plans)

Recovery SharePoint Site Contents:

- IT recovery invocation procedures
- Managers contact list (including subcontractor contacts)
- Suppliers and delivery partner contact list
- Pre-prepared statements and recipient lists
- Insurance broker contact details

14.6 IMT Infrastructure Needs

Item	Quantity/timeframes				
	1 day	3 days	5 days	2 wks.	>4 wks.
Desks, PCs	1	0	0	0	0

Where the IMT operates remotely or from alternative sites, secure remote IT access and communications are provided to all team members and relevant subcontractor leads.

14.7 IMT Action plan

Day 1 – Actions	Status
Contact SLT leader, brief on current position and agree initial strategy. Agree on timings of next updates.	
Obtain SLT approval to invoke recovery contracts	
IT Recovery Team (ITTRT) leader to invoke recovery site and IT emergency supplier contracts. Establish when the minimum required configuration will be ready for occupancy.	
Ensure staff involved in the salvage operation have adequate briefings, advice and support	
Ensure H&S regulations are not contravened at any stage of the crisis	
Nominate a team member to attend site as soon as possible	
Arrange extra security for premises	
INCIDENT DURING WORKING HOURS: the IMT has responsibility for the evacuation of the building(s), in conjunction with the fire wardens.	
Liaise with emergency services. Provide them with staff lists and contact details of recovery teams. Establish when access to site will be possible	
Establish a co-ordination centre and communicate details to the business and to the emergency services	
Obtain SLT approval to send home non-essential personnel if the building cannot be re-entered. Instruct personnel to await further instructions and ensure they leave contact numbers.	
Contact all departmental managers to obtain a list of missing persons and known casualties. Communicate situation to SLT.	
Ensure that the recorded message has been installed on all incoming voice lines	
Decide location and time of IMT meetings. Agree composition of team.	
Retrieve off-site Recovery SharePoint Site	
Initiate damage assessment operation as soon as access to the site is permitted. Photograph or video damage before salvage begins, for insurance purposes.	
Arrange additional security staff to secure building and arrange access control.	
Arrange a visit of the loss adjusters. arrange a visit of the loss adjusters.	

Days 2-3 – Actions	Status
Engineers to provide an assessment of the damage.	
Hold status update meetings with other recovery teams and communicate status to SLT	
Hold status update meetings with other recovery teams and communicate status to SLT	
Confirm that IT and business operations at the recovery site are established	
Continue liaison with emergency services, SLT, ITTRT and insurance company	
Receive any unexpected business visitors at the co-ordination centre and advise them of new business contact arrangements.	

Days 4-5 – Actions	Status
Agree purchasing and budgetary limits with insurers. Authorise placement of orders/ invocation or emergency procurement agreements for equipment	
Continue liaison with emergency services, SLT, ITTRT, insurance company and Divisional Directors	

Days 5-28 – Actions	Status
Continue contact with salvage company, structural engineers and landlord to review status of damage	
Consolidate damage assessment and salvage reports and communicate to SLT	
Meet with loss adjuster and insurance company representative to establish the basis for submitting the insurance claims	
Obtain an update on the financial position. Assess recovery expenditure outlay to date.	
Investigate rebuilding timescales, costs, level of insurance claim	
If the building will not become habitable within one month, meet with property services to plan longer-term recovery options. Otherwise, initiate reconstruction and refit, also investigate availability of local office space for short-term rental.	
Liaise with recovery team leaders to develop long-term recovery plan	

15. IT Recovery Plan

15.1 IT Recovery Team Plan

The IT Recovery Team (ITRT) is responsible for restoring IT, telecommunications, and digital services following any disruption affecting Twin operations. This includes services delivered directly, via the Twin English Centre Ireland (TECI), and through subcontracted or partner organisations.

Most Twin systems are cloud-hosted, ensuring continuity even if physical sites are unavailable. A small number of systems remain onsite in Greenwich (e.g., Sage 50, PO DB, GT DB) and require recovery actions as defined in this plan.

Telecommunications are hosted via MS Teams, so in the event of internet outages or cyber incidents, all Incident Team, Recovery Team, and SLT members will use MS Teams telephony.

Recovery plans consider TECI operational systems and subcontracted service delivery to ensure minimal disruption for learners, staff, and partners.

15.2 ITRT Responsibilities

The ITRC ensures a secure, safe, and efficient IT and business recovery environment across all Twin sites, including TECI, and where subcontracted delivery is involved.

Key responsibilities include:

- Coordinating IT recovery with the Incident Management Team (IMT) and Senior Leadership Team (SLT)
- Preparing recovery sites and remote access arrangements for both Twin and TECI operations
- Retrieving off-site IT resources and critical assets
- Reconstructing IT systems, telecommunications, and support services at recovery sites
- Ensuring subcontracted partners and TECI staff can continue delivery with minimal interruption
- Liaising with suppliers, subcontractors, and service providers to restore infrastructure efficiently
- Ensuring all staff involved in recovery are aware of support arrangements and security protocols
- Maintaining overnight security for temporary IT recovery resources
- Assisting with damage assessment and updating internal and customer-facing digital systems

Infrastructure recovery objectives	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks.	>4 wks.
Liaise with Incident Management Team (IMT) and Senior Team (SLT)	1	0	0	0	0
Prepare recovery site according to priority of business functions as defined by SLT	1	0	0	0	0
Retrieve off site resources	1	0	0	0	0
Telecommunications redirection	0	0	0	0	0

Reconstruct IT and Telecommunications requirements at recovery site	1	0	0	0	0
Reconstruct critical premises requirements at recovery site	1	0	0	0	0
Reconstruct support services at recovery site	1	0	0	0	0
Liaise with DR IT and equipment suppliers	1	0	0	0	0
Ensure business recovery staff are aware of support arrangements	1	0	0	0	0
Ensure temporary IT recovery resources are secure overnight – security guard required?	1	0	0	0	0
Assist with damage assessment	1	0	0	0	0
web site for customer information	1	0	0	0	0

15.4 ITRT Team Location

The IT Recovery Team recovery site will normally be:

- Southwark Centre – 224–236 Walworth Road, 4th Floor, Manor House, London SE17 1JE
- Greenwich Centre – 12 Lambarde Square, Greenwich SE10 9GB
- Local offices or home-based if primary sites are unavailable

The team will determine the operational site at the time of the incident based on the nature and location of the disruption.

Recovery plans explicitly include TECI operational continuity and subcontractor-supported sites, ensuring all essential IT and communications services are restored wherever delivery occurs.

15.5 ITRT Team Members

Name	Department / Title	Function	Contact details
Morné Du Toit	Director of IT	Deputy Leader Hardware and Software Rebuild	07772003045
Otis Kotsanos	IT Support Manager	Users' setup	07798836167

15.6 ITRT Vital Records

The IT Recovery Team's SharePoint Site is maintained securely on the cloud. Paper copies are stored at:

- Greenwich Centre, 12 Lambarde Square, Greenwich SE10 9GB
- Southwark Centre, 224–236 Walworth Road, 4th Floor, Manor House, SE17 1JE
- Equivalent operational documentation is maintained for TECI and all subcontracted delivery partners to ensure continuity of service, systems access, and recovery coordination.

Recovery SharePoint Site Contents:

- IT Disaster Recovery Plan
- Key contact lists (suppliers, subcontractors, stakeholders)
- System passwords
- List of staff authorised to invoke IT recovery procedures
- DR IT invocation procedures
- DR IT recovery site location maps
- Asset list

15.7 ITRT System Needs

Group	Quantity/timeframes				
	1 day	3 days	5 days	2 wks.	>4 wks.
SLT	1	0	0	0	0
IMT	1	0	0	0	0
IT	1	0	0	0	0

Group	Quantity/timeframes				
HR	1	0	0	0	0
Communications	1	0	0	0	0
Finance	1	0	0	0	0
Repairs	1	0	0	0	0
Total	1	0	0	0	0

15.8 ITRT Action plan

Day 1 - Actions	Status
All systems are SAAS cloud systems with failovers in place. No events at Twin sites will affect this uptime.	
Cloud telephony is also used -Teams telephony is used so no physical phone systems with downtime risk	
Verify connectivity and access for remote staff, including TECI and subcontracted delivery teams.	
Notify all operational teams of incident response status and expected IT support channels.	
Confirm security monitoring (firewalls, server alerts, antivirus) is active and logging events.	
Validate backup systems and offsite storage integrity for critical data (including TECI and subcontracted systems).	
Establish IT helpdesk contact points for staff and subcontractor queries during the incident.	

Days 2-14 - Actions	Status
Restore and verify any on-premise systems that are affected (e.g., Sage 50, PO DB, GT DB).	
Implement temporary access solutions for staff and subcontractors if primary sites are unavailable.	
Conduct system integrity checks for cloud and on-premise applications, including TECI operational systems.	
Coordinate with IMT to ensure all systems required for continuity of teaching, student management, and partner communications are operational.	
Apply any required security patches or updates to IT infrastructure.	
Test telephony failover and MS Teams call routing to ensure continuous communications across all sites.	
Document all recovery steps, communications, and system changes for audit and reporting purposes.	
Support subcontracted partners in restoring their IT-dependent services and ensure alignment with Twin's recovery strategy.	
Conduct staff training/refresher if new access procedures or tools are implemented.	

Days 14-28 - Actions	Status
Complete post-incident review of all systems, including TECI and subcontractor IT operations.	
Validate that backups, failovers, and cloud redundancy systems meet continuity requirements.	
Implement improvements to IT recovery processes based on lessons learned from the incident.	
Restore full functionality to any systems still in temporary mode or offline during short-term recovery.	
Coordinate with SLT and IMT to verify operational reporting, monitoring dashboards, and student/partner access are fully restored.	
Coordinate with SLT and IMT to verify operational reporting, monitoring dashboards, and student/partner access are fully restored.	
Review cybersecurity posture and update policies or tools to mitigate future risks.	
Plan and implement additional resilience measures for subcontracted delivery partners and TECI operations.	
Conduct internal audit of recovery actions and infrastructure usage during the incident.	

15.9 ITRT Systems restoration

System	Timeframes				
	0 day	1 days	5 days	2 wks.	>4 wks.
E-mail – Office 365 cloud and mime cast	0	0	0	0	0
TET uses multiple cloud-based solutions	0	0	0	0	0
File data in MS Teams and SharePoint	0	0	0	0	0
People HR	0	0	0	0	0
Bullhorn, Salesforce CRMs	0	0	0	0	0
Sage 50 accounts	0	0	0	0	0
Phone systems	0	0	0	0	0
Intranet - SharePoint	0	0	0	0	0

16. HR Team

16.1 HR Team Recovery Plan

The HR Team is responsible for strategic oversight and coordination of all HR activities during the invocation of the BCDRP. This includes ensuring the continuity of payroll, staff welfare, counselling, and the management of any staff issues that arise during an incident.

The HR Team also supports operational capacity planning, informed by monthly Business Reviews, and ensures that HR functions for TECI and subcontracted delivery partners are maintained. This includes communication, payroll, and welfare processes for staff located across Ireland, the UK, and third-party partner organisations.

16.2 HR Team Responsibilities

The HR Team ensures:

- Staff welfare is prioritised, including for families or colleagues affected by serious injury or fatality.
- Confidentiality of all personnel records is maintained.
- Payroll and HR administrative functions continue without disruption.
- Timely communication with staff regarding expenses, welfare, and operational updates.
- Liaison with the Incident Management Team (IMT), Emergency Response Teams, and subcontracted partners to ensure HR continuity.
- Support for TECI operations, ensuring staff and student-facing teams receive guidance and HR support.

HR recovery objectives	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks.	>4 wks.
Deal with the welfare of staff, particularly for families and colleagues of staff who have suffered major injury or fatality	1	0	0	0	0
Regular contact with non-recovery staff	1	0	0	0	0
Activate counselling where appropriate	2	0	0	0	0
Provide regular briefings for all staff about expenses / payments / welfare	1	0	0	0	0
Maintain contact with finance team and submit payroll information for processing	1	0	0	0	0
Maintain confidentiality of personnel records	1	0	0	0	0
Liaise with Incident Management Team and Emergency Management Teams	1	0	0	0	0

16.3 HR Team Location

At the time of the incident, the HR Team will agree a temporary operational site near the Greenwich HQ or Southwark Centre.

Remote operation will be supported for TECI staff and subcontractors if physical locations are inaccessible.

Primary Recovery Sites:

- Southwark – 224–236 Walworth Road, 4th Floor, Manor House, London SE17 1JE
- Greenwich HQ – 12 Lambarde Square, London SE10 9GB
- Dublin English Centre (TECI) – local operational site if required
- Remote/home-based operation for staff and subcontractors

Name	Department / Title	Function	Contact details
Joanne Sayer	Chief People Officer	Staff Leadership	07950984660
Jacqui Fox	Director, Strategic Partnerships	Staff Leadership	07740540079
Jose Pacheco	Financial Controller	Staff Leadership	07535058287

16.4 HR Vital records

The HR Team's critical records are maintained on People HR and Recovery SharePoint Sites. Secure paper copies are stored at:

- Southwark – 224–236 Walworth Road, 4th Floor, Manor House, London SE17 1JE
- Greenwich HQ – 12 Lambarde Square, London SE10 9GB
- TECI – Dublin site (local copy for continuity of staff operations)

16.5 HR Recovery SharePoint Site contents:

Recovery item	Status
Next of kin details	
List of staff with PC access from home	
List of bank staff	
HR contacts list – payroll, pension, counselling and legal advisors	
Contact lists for additional staff: local Centre Managers, sub-contractors and stakeholders	
Answerphone draft message	

16.6 HR Infrastructure needs

Item	Quantity/timeframes				
	1 day	3 days	5 days	2 wks.	>4 wks.
Desks, Mobiles, Ms Teams, PCs	1	0	0	0	0

16.7 HR Systems requirements

System	Timeframes				
	1 day	3 days	5 days	2 wks.	>4 wks.
e-mail	1	0	0	0	0
HR system	1	0	0	0	0
Excel data files	1	0	0	0	0

16.8 HR Action plan

Day 1 - Actions	Status
Deal with the welfare of staff, particularly for families and colleagues of staff who have suffered major injury or fatality	
Direct all staff who are not immediately required to return home and stay by phone until contacted. Before leaving site, all staff are responsible for checking in with HR team members or line manager to confirm contact details (phone and e-mail) and immediate strategy	
Team members begin to maintain HR group whereabouts log on a daily basis	

Day 1 - Actions	Status
Agree short term recovery location. Communicate location and contact details to the IMT. Relocate recovery team to short term location	
Hold initial planning meeting. Make contact with the IMT and report immediate status. Agree time and venue of next meeting	
Meet with heads of departments to redeploy staff from the group business and other centres & ensure succession planning strategies are implemented	
Contact stress counsellors and put them on standby	
Advise essential contacts of situation and contact details	
Work closely with IMT and Divisional Directors to ensure staff welfare issues are given high priority	
Relocate 1 member of the team to the recovery site as soon as it is ready for occupancy	
Ensure that staff details are made available to the IMT and emergency health services when appropriate	
Obtain mobile phone – either one that is available or buy a pay-as-you-go phone for incoming calls and recorded HR message only	
Check that staff communications procedures are in place (recorded message giving status and high-level guidance to staff, always giving next time of update)	

Days 2-3 – Actions	Status
Continue to deal with the welfare of staff, particularly for families and colleagues of staff who have suffered major injury or fatality	
If there is a large loss of staff, review workload to core and non-core activities and services. Redeploy available staff where possible	
Consider options to meet additional staff requirements: other local centres and sub-contractors	
Relocate HR recovery team to recovery site as soon as it is ready. Set up HR helpdesk and publicise contact numbers to all staff and sub-contractors. Try to ensure helpdesk is in a quiet or private location	
Advise staff of stress counsellors' contact details	
Ensure status update line is operational, not overloaded, and that a mechanism is in place to regularly update the message. In each message state when the next update will be and advise staff to keep trying if the number is engaged	
Continue regular communication with IMT and departmental heads	
Book Ms Teams meetings for regular staff updates. Arrange to hold first meeting today, if possible	
Draft a communication for all staff explaining how expenses should be claimed by staff attending the recovery site. Reassure them that a business continuity plan is in place and that recovery to normal will occur as quickly as possible. Give contact numbers for HR helpline and the status update line. Tell staff when the staff update meetings will take place	
Communicate with HR legal advisors Mentor	
If outage occurs when payroll is due, contact the bank and request them to run the payroll based on last month's figures. Draft letters for staff explaining the pay arrangements for this month and outline the types of adjustments that will be made to their pay for next month.	

Days 4-28 – Actions	Status
Continue to deal with the welfare of staff, particularly for families and colleagues of staff who have suffered major injury or fatality	
Continue to hold regular meetings with all staff	
Continue to provide support to staff via the stress counsellors and the HR helpdesk at the recovery site	
Continue regular communication with IMT and departmental heads	
Contact all team members and confirm ongoing contact arrangements. Communicate status of wide recovery to HR team	
Maintain contact with HR supplier	
Longer term assessment of contract staffing needs and recruitment processes	

17. Finance Team

17.1 Finance Team Recovery Plan

The Finance Team is responsible for managing and coordinating all financial activities associated with the invocation of the BCDRP. This includes ensuring continuity of financial operations, maintaining cash flow, processing payments, and supporting operational teams during any disruption affecting Twin operations.

Twin's accounting and financial data are primarily held within Sage, Class, and the Twin server environment, with backups managed through the IT infrastructure as outlined in the IT Recovery Plan. As the organisation operates a largely paperless finance system, the risk of data loss is minimal. In the event of a physical incident affecting office locations, only documents received but not yet scanned may be temporarily unavailable.

The Finance Team's recovery arrangements support all financial operations across Twin, including TECI (Twin English Centre Ireland) and services delivered through subcontracted partners and delivery organisations. Financial continuity includes managing funding claims, supplier payments, payroll, and contractual payments relating to partner delivery arrangements.

17.2 Finance Team Responsibilities

The Finance Team is responsible for supporting the organisation's financial stability and ensuring the continuation of essential financial operations during a major incident.

Key responsibilities include:

- Coordinating financial recovery activities with the Incident Management Team (IMT) and Senior Leadership Team (SLT)
- Maintaining operational cash flow to support organisational continuity
- Ensuring payroll and other essential payments continue without disruption
- Managing payments to suppliers, subcontractors, and partners
- Supporting financial reporting requirements for commissioners and stakeholders
- Maintaining financial records and ensuring their secure recovery where required
- Ensuring continuity of billing, invoicing, and receipt collection from customers and partners
- Supporting TECI operations and subcontracted delivery partners in maintaining financial processes during disruption

Finance recovery objectives	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks.	>4 wks.
Liaise with Incident Management Team (IMT) and Senior Team (SLT)	1 day	0	0	0	0
Send communication and update to relevant stakeholders about the incident and progress	1 day	0	0	0	0
Provide operational cash flow	0	0	0	2 wks.	0
Restore facility to bank cheques and issue funds via BACS or other means	0	3 days	0	0	0
Recover /recreate and maintain financial records	0	0	5 days	0	0
Set up facility for requesting payment cards	0	0	5 days	0	0
Release payments to suppliers	0	0	0	2 wks.	0
Ensure continuity of billing and collection of receipts from respective customers	0	0	5 days	0	0
Ensure payroll and other necessary business payments are continuing	0	0	5 days	0	0
Monthly / quarterly reports	0	0	0	2 wks.	0

17.4 Finance Team Location

At the time of an incident, the Finance Management Team will determine the most appropriate operational location depending on the nature of the disruption.

The team may operate from:

- **Greenwich Headquarters** – 12 Lambarde Square, London SE10 9GB
- **Southwark Centre** – 224–236 Walworth Road, 4th Floor, Manor House, London SE17 1JE
- **Remote/home-based locations**, where systems access allows continuity of financial operations

Remote working capability ensures the Finance Team can continue supporting TECI operations and subcontracted partners, ensuring payments, claims, and financial processes remain operational.

17.5 Finance Team Members

Name	Department / Title	Function	Contact details
Jose Pacheco	Financial Controller	Deputy Leader	0208 269 5686; 07535058287
Deirdre Lensley	Accounts Assistant	Accounts Payables	0208 269 7533

17.6 Finance Vital records

The Finance Team's critical documentation is maintained electronically via the Finance Recovery SharePoint Site. Secure access is maintained across the organisation to ensure continuity during an incident.

Temporary access to recovery documentation may also be provided through the Southwark Centre if required.

Recovery documentation supports financial operations across Twin, TECI, and subcontracted delivery partners, ensuring that financial processes remain operational during any disruption.

17.7 Finance Recovery SharePoint Site contents

Recovery item	Status
Manual cheque books for payment of suppliers and expenses	
Paying in books for the main bank accounts	
List of authorised cheque signatories	
BACS bureau number & pin	
List of bank accounts	
Standard forms (expense claim, cheque requisition)	
Key contact list	
Full staff contact list and staff chart for Finance	
Details of all sub-contractor and funding agency, bank and contact details	
Deadlines, Service Standards and Checklists	
Contract working capital requirements	

17.8 Finance Infrastructure needs

A secure location for financial materials, including a safe for petty cash, will be maintained if required.

Item	Quantity/timeframes				
	1 day	3 days	5 days	2 wks.	>4 wks.
Desks, PCs	1	0	0	0	0
Banking and Payments tools, log ins	1	0	0	0	0

17.9 Systems requirements

System	Timeframes				
	1 day	3 days	5 days	2 wks.	>4 wks.
Sage System	1	0	0	0	0
Access to all Government related claims systems such as TTS, Pics, Bravo, e-Claims	1	0	0	0	0

PICs/Class/CRM	1	0	0	0	0
e-mail and Microsoft Office	1	0	0	0	0
Bank Account Access	1	0	0	0	0
Access to the server	1	0	0	0	0

17.10 Finance Action plan

Day 1 – Actions	Status
Required to return home and stay by phone until contacted. Before leaving site, all staff are responsible for checking in with Finance team leaders to confirm contact details and immediate strategy contact details and immediate strategy	
Team leaders begin to maintain group whereabouts log on a daily basis	
Agree short term recovery location. Communicate location to Senior Team (SLT). Relocate recovery team to short term location.	
Hold initial planning meeting. Make contact with Senior Team (SLT) and report immediate status. Agree time and venue of next meeting.	
Advise essential contacts of situation and contact details.	
Obtain confirmation from SLT as to when recovery site will be ready for occupancy	
Prepare Banking and Payments recovery team to relocate to recovery site as soon as it is ready. Liaise with SLT to agree staff transport details	
Contact all team members and confirm ongoing contact arrangements. Communicate status of firm-wide recovery to all staff.	
Relocate Banking and Payments recovery team to recovery site as soon as it is ready. Team focuses on making payments to enable operations to continue	
Contact all commissioners as appropriate	

Days 2-3 – Actions	Status
Evaluate the effect of any lost transactions on business operations	
Continue regular communication with SLT. Establish condition of financial records and General Ledger	
Contact all team members and sub-contractors confirm ongoing contact arrangements. Communicate status of firm-wide recovery to all staff.	
Review the next deadlines for Management Accounts to produce company reports, and prepare to relocate one member of the team to the recovery site if required	
By the end of Day 3, extend Banking and Payments functions to include management of operational cash-flows and payment of suppliers	
Locate cash receipts to recovery site.	

Days 4-5 – Actions	Status
Representative to the recovery site and commence production of reports or reconstruction of financial records or reconstruction of financial records	
Continue Banking and Payments activity as Days 1,2-3.	

Days 4-5 – Actions	Status
Continue regular communication with SLT.	
Contact all team members and confirm ongoing contact arrangements. Communicate status of firm-wide recovery to all staff.	
Continue cash receipt activity	

Days 5-28 – Actions	Status
Continue as Days 4-5	
Re-assess requirement for Management Accounts to produce reports, if they have not already been relocated to the recovery site	
Relocate member of Management Accounts to recovery site, if not already there. Commence production of reports and reconstruction of financial records.	

18. Facilities Team

18.1 Facilities Team Recovery Plan

The Facilities Team is responsible for coordinating the physical infrastructure and operational environment required to support the recovery of Twin operations following a disruption. This includes ensuring that safe, secure, and suitable premises and operational resources are available to support staff, learners, and delivery partners during the recovery process.

Facilities recovery arrangements apply across all Twin operational sites, including the Twin English Centre Ireland (TECI) and any locations used by subcontracted delivery partners. Where incidents affect physical premises, the Facilities Team will work with operational leaders to identify suitable alternative arrangements and ensure that critical services can continue.

The Facilities Team works closely with the Incident Management Team (IMT) and Senior Leadership Team (SLT) to prioritise recovery of premises and infrastructure based on operational needs, learner welfare, and contractual delivery requirements.

18.2 Facilities Team Responsibilities

The Facilities Team ensures that appropriate resources and facilities are available to support operational recovery.

Key responsibilities include:

- Liaising with the Incident Management Team (IMT) and Senior Leadership Team (SLT) regarding facilities requirements during recovery
- Preparing recovery sites according to the priority of business functions defined by SLT
- Reconstructing or restoring critical support services at recovery locations
- Ensuring staff involved in recovery operations are aware of facilities arrangements and support services
- Supporting TECI and subcontracted partners where facilities or delivery locations are affected
- Assisting with damage assessment of operational premises
- Ensuring temporary facilities and recovery resources remain secure

Facilities recovery objectives	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks.	>4 wks.
Liaise with Incident Management Team (IMT) and Senior Team (SLT)	1	0	0	0	0
Prepare recovery site according to priority of business functions as defined by SLT	1	0	0	0	0

Reconstruct support services at recovery site	1	0	0	0	0
Ensure business recovery staff are aware of support arrangements	1	0	0	0	0
Ensure temporary recovery resources are secure overnight – security guard required?	N/A	0	0	0	0
Assist with damage assessment	1	0	0	0	0

18.3 Facilities Team Location

At the time of an incident, the Facilities Management Team will determine the most appropriate operational location based on the nature and location of the disruption.
The team will normally operate from:

- Southwark Centre – 224–236 Walworth Road, 4th Floor, Manor House, London SE17 1JE
- Greenwich Headquarters – 12 Lambarde Square, London SE10 9GB
- Other operational locations where required

Where operational premises are affected, the Facilities Team will support arrangements for TECI operations and subcontracted delivery sites, ensuring alternative premises or operational facilities are identified where necessary.

Name	Department / Title	Function	Contact details
Joanne Sayer	Chief People Officer (also responsible for Facilities)	Office Infrastructure Management	07854 250911

18.4 Facilities Vital records

The Facilities Team maintains key operational documentation through the Facilities Recovery SharePoint Site, which is securely stored electronically and accessible to authorised staff.

Paper copies of critical documentation may also be held at the Southwark Centre where required. The documentation supports operational oversight across Twin sites, TECI operations, and subcontracted delivery premises.

18.5 Facilities Recovery SharePoint Site contents:

Recovery item	Status
Suppliers contact list	
Business continuity plan	
Emergency contact list: security, transport, stationery	
List of all operational premises	
List of and contact details for all keyholders for operational premises	
List of and contact details for most senior managers located at all operational premises	
List of all relevant local Royal Mail sorting offices with contact details	

18.6 Facilities Infrastructure needs

Item	Quantity/timeframes				
	1 day	3 days	5 days	2 wks.	>4 wks.
Desks, Telephones, PCs	0	0	1	1	1

18.7 Facilities Action plan

Day 1 – Actions	Status
Retrieve Recovery SharePoint Site	
Investigate shuttle bus arrangements for staff transport to recovery site	
Advise IMT of progress	
Ensure recovery staff are aware of support arrangements	

Days 2-14 – Actions	Status
Assist as required with salvage operation	
Arrange for staff to collect mail from sorting office (for security reasons)	
Advise all essential contacts including sub-contractors of situation and new contact details	
Review office equipment installed at the recovery site jointly with Twin IT to agree optimal recovery situation	
Continue to report progress to IMT	
Assist IMT with damage assessment	
Provide assistance to other recovery teams as requested	
Provide support services to recovery staff	
Ensure that the reception staff are aware of staff locations and have telephone numbers for local courier companies	

Days 15-28 – Actions	Status
Continue as Days 2-14	
Assist in the recovery of main office site	
Begin to prepare for return home. Inspect site, review salvaged equipment, agree purchasing requirements, produce project plan	

19. Plan Review and Maintenance

19.1 Updating the Plan

This section outlines the procedures for reviewing, updating, and maintaining the BCDRP to ensure it remains accurate, effective, and aligned with organisational operations.

The responsibility for updating recovery procedures sits with each Business area, it must ensure that the relevant sections of the plan reflect current operational arrangements. This includes services delivered directly by Twin, through the Twin English Centre Ireland (TECI), and through subcontracted or partner organisations involved in programme delivery.

A governance structure is in place to ensure that the plan remains current and effective. This includes procedures to:

- Authorise the removal or updating of recovery procedures held within distributed versions of the BCDRP.
- Maintain a formal record of all updates and revisions to ensure the most recent version of the plan is in use
- Conduct periodic audits of distributed copies to ensure version integrity across the organisation

All team members have a responsibility to notify their HoBU of any changes to information contained within the plan. This includes updates relating to:

- Preferred suppliers
- Subcontracted delivery partners
- Operational sites, including TECI locations
- Key staff contact details
- Emergency contact information

19.2 Plan Review Process

To ensure the plan remains accurate and operationally effective, the following activities will be undertaken on a regular basis:

- Conduct a structured plan walkthrough or simulation exercise involving relevant staff and managers to identify any changes in working practices since the previous review
- Confirm that only the current approved version of the plan is in circulation
- Update any outstanding actions or “open issues” identified during reviews or testing exercises
- Communicate updates or amendments to all relevant staff and operational teams

19.3 Distribution

An up-to-date version of the BCDRP is maintained and distributed as follows:

- An electronic version is held on Twin Microsoft Teams, accessible to authorised staff
- All individuals referenced within the plan must have access to the document, including the current version number and date of issue
- Relevant operational leads supporting TECI operations and subcontracted delivery partners will also have access where appropriate

The distribution list is reviewed monthly to ensure:

- All relevant personnel retain access to the plan
- Access is removed from individuals who leave the organisation
- Updated copies are circulated when amendments are made

19.4 Version Control

Each page of the BCDRP contains a version number and page number.

When any part of the plan is amended and redistributed:

- The previous version must be securely destroyed using the same procedures applied to confidential documents
- Sign-off must be obtained from the relevant HoBU to confirm that their section has been reviewed and remains accurate

19.5 Update Schedule

The BCDRP should be updated:

- When major changes take place, e.g., changes in structure, customer base or business roles
- After tests, to incorporate any new information which may come to light.
- Routinely, at the following intervals:

Category	Rec. Update frequency	Update responsibility	Last updated	
			Name	Date
Review business risks	6 monthly	SLT	Debra Jackson	
Review impact analysis	6 monthly	SLT	Debra Jackson	
Review critical IT systems	3 monthly	Director of IT	Morné Du Toit	
Staff details (home phone numbers)	Monthly	HR/Managers	Joanne Sayer	
Vital records	3 monthly	HR/Managers	M Joanne Sayer, Morne Du Toit	
Internal contacts/ dependencies	3 monthly	Function Managers	Gemma Clarke / Lynsey Whitehead	
External contacts	3 monthly	SLT/ Function Managers	Jose Pacheco	
Recovery requirements	6 monthly	SLT	Debra Jackson	
Recovery location details	6 monthly	Director of IT	Morné Du Toit	
Any other details likely to change regularly	3 monthly	Operational Managers/Director of IT	Gemma Clarke Lynsey Whitehead Morné Du Toit	

When updates are made to the plan, any teams or functions that may be impacted (for example, IT or operational teams) will be informed to ensure alignment and effective implementation of the changes.

As a minimum, all sections of the plan will be reviewed and updated annually, or sooner where required following a critical incident, significant organisational change, or other milestone that may affect the arrangements outlined within the plan.

19.6 Maintenance lists

19.6.1 Senior Management Team

Activity	☐ Box
Review and confirm with the Incident Management Team the business continuity and disaster recovery arrangements. Confirm the recovery strategy.	
Revisit the Business Impact Analysis to re-establish and confirm priorities	
Review and implement additional testing scenarios such as cyber security hackathon	

19.6.2 Incident Management Team

Activity	☐ Box
Regularly review and ensure any standby services likely to be used are adequate and still usable.	
Ensure regular reviews of the Plan and recovery strategy are carried out with all Recovery Team Leaders.	
Make every effort to carry out a user test at least once per year. If this is not possible conduct a 'walk-through' of the plan.	
Make sure the software and data back-up and off-site storage arrangements are satisfactory.	
Ensure insurance cover is sufficient for any likely disaster scenarios.	
Be aware of all critical customer services and the possible standby/fall-back options available.	
Advise users on the necessity to maintain up to date emergency clerical procedures or other standby services for critical activities that are needed to deal with a technology service only disaster.	
Identify and maintain procedures to deal with personnel issues related to a disaster. This should include trauma, loss of life, communications with relatives, knowledge of where to acquire temporary staff and schedules of personnel based at each location.	

19.6.3 IT Team

Activity	☐ Box
Maintain details of the minimum requirements for office furniture and other office equipment, not provided as part of the standby service.	
Keep details of space requirements for use in determining a suitable location at the time of a disaster.	
Keep details of office furniture and office equipment for total replacement at the time of a disaster.	
Maintain regular contact with suppliers, manufacturers, leasing companies and brokers and, where possible, seek an understanding from them about lead times for the rapid delivery of services and products, at the time of an emergency.	
Ensure all data and software is backed up and that the most recent copy possible is kept securely at an offsite store.	
Ensure that records are maintained of security codes, machine IDs, etc. necessary to run all operating and applications software.	
Ensure that a copy of essential reference material, procedure manuals, operations manuals, etc. is held off site and checked from time to time to ensure the correct and up to date issue is available.	
Maintain restore procedures for all computers and periodically do penetration tests. Occasionally use less experienced staff to perform the restore rather than key individuals.	

Activity	□ Box
Ensure all details relating to any standby services are maintained up to date - invocation details, equipment specifications, restore procedures, etc.	
In conjunction with the users, carry out periodic tests of the standby services and document the results. Do this at least every six months and whenever there are significant changes in hardware/software at either location.	
Keep details of telephony recovery up to date. Make sure telephony recovery documentation is maintained up to date.	
Maintain the standby centre desk / business function layout up to date.	
Agree and record priorities for re-establishing IT services at the standby location.	
Be aware of any additional equipment required, over and above that provided at the standby site, and where this can be sourced.	
Make sure 'out of hours' contact details for all employees are readily available at all times.	
Review additional Security/Data protection/Cyber testing	

19.6.4 Business Functions

Activity	□ Box
Confirm the standby resources needed to support the agreed critical activities in an emergency situation.	
Consider any additional control procedures that may be necessary in the event of a disaster.	
Develop any special procedures needed to ensure good accounting practices at the time of a disaster.	
Be aware of the procedures for controlling additional expenditure at the time of a disaster.	
Work with other members of the business teams on the preparation of any specific emergency manual procedures needed to support the standby facilities.	

20. Testing

Testing is an essential component of ensuring that the objectives set out in the BCDRP can be achieved in practice. Regular testing provides assurance that recovery arrangements are effective, roles and responsibilities are clearly understood, and that systems and processes will operate as intended in the event of a disruption.

Testing also provides a valuable development and training opportunity for staff involved in business continuity activities, helping to strengthen organisational readiness and response capability.

All testing activities will be carefully planned and coordinated to minimise disruption to normal business operations while maximising the learning and assurance gained from the exercise. Where appropriate, testing may include participation from relevant operational areas, including Twin English Centre Ireland (TECI) and subcontracted delivery partners, particularly where their services form part of critical operational or delivery functions.

This section outlines the methods by which the Twin Business Continuity Plan will be tested, reviewed, and strengthened over time.

Description	Objective	Test frequency	Last test
IT test at recovery site	• To verify that critical IT systems can be successfully restored and accessed from the recovery environment • To confirm that cloud systems, data backups, and failover arrangements operate as expected during a disruption • To ensure staff can securely access key systems (e.g., email, Teams, and operational platforms) from the recovery location or remotely • To validate that IT recovery procedures support the continuation of core business operations, including TECI delivery and subcontracted provision where relevant	6 monthly	Feb 2025
Tabletop test with recovery teams	• To ensure staff are aware of their responsibilities • To highlight flaws with the plans so that they may be corrected. • To always be prepared for emerging cyber risks	6 monthly	Feb 2025
IT recovery and recovery teams at recovery site	• Simulate 'real' disaster situation including penetration tests to pull all teams together.	Yearly	Feb 2025

21. Sample Media Statements

21.1 Media statement

In the event of a major incident affecting Twin operations, any communication with the media must be carefully managed to ensure accuracy, consistency, and the protection of individuals and the organisation.

Official media statements will only be issued by the Chief Executive Officer, Chief People Officer, or another member of the Senior Leadership Team (SLT) designated by the SLT at the time of the incident.

If approached by journalists or members of the media before an official statement has been issued, staff should not provide comment and should instead refer enquiries to the designated SLT spokesperson.

21.2 Initial Holding Statement

In the early stages of an incident, the following type of holding statement may be used:

[Name of company]

As a result of a nearby [*gas explosion/bomb threat*] within the vicinity of Main office site, the premises of Twin have been temporarily evacuated. This is a standard procedure taken on the advice of local emergency services in the interests of public health and security.

Twin has developed a sophisticated "business continuity plan" for use in such instances. This has enabled us to limit the damage/inconvenience caused by this unexpected event.

This plan includes having a contingency site from which Twin can become fully operational within 48 hours and minimise the effect to our customers. Within this site, based in Lewis Grove, Lewisham all systems functions and telecommunications will be established – ensuring that there is a seamless resumption of business as usual.

Advanced planning means that all of Twin computer systems are fully backed, and no transactional data will be lost. Consequently, there will be no adverse effect to customers and their accounts with us.

All customers and business partners will be informed of the situation in writing and reassured that there is nothing for them to be concerned about.

ith the emergency services and resume work in main office site as soon as it is confirmed to be safe for all parties. We anticipate this to be within the next 24 hours and will of course keep you informed at all times. course keep you informed at all times.

21.3 Example Media Questions and Responses

1. What caused the incident and when did you first become aware of it?
The cause of the incident has not yet been confirmed. The relevant authorities are currently investigating and we are fully cooperating with them. Twin was notified of the situation promptly and our established emergency and business continuity procedures were immediately implemented.

2. Who is responsible for what happened?
We are unable to comment on responsibility at this stage. Any investigation is being managed by the relevant authorities and it would be inappropriate to speculate while that process is ongoing.

3. You appear confident that operations will resume quickly. Were you expecting this to happen?
While incidents of this nature cannot be predicted, Twin maintains a comprehensive Business Continuity Plan to ensure that we can respond quickly and effectively to unexpected events. These procedures are designed to protect people, maintain essential operations, and minimise disruption to learners, staff, and partners.

4. Will learners, customers, or partners be affected?
Our immediate priority is ensuring the safety of everyone involved. At the same time, our recovery procedures have been activated to minimise disruption to services. We have contingency arrangements in place that allow key operations to continue, including remote working capabilities and alternative delivery arrangements where required.

5. Were there any casualties?
At this stage we are working closely with the emergency services who are managing the situation. Our focus remains on the safety and wellbeing of everyone involved. Any confirmed information will be shared once it has been verified by the appropriate authorities.

21.4 Media Handling Guidelines

During any incident, all staff should follow these communication principles:

Key Messages
Communications should focus on the following messages:

- The safety and wellbeing of staff, learners, and visitors is the organisation's highest priority
- Emergency services and relevant authorities are managing the incident where appropriate
- Twin has activated its Business Continuity and Recovery procedures
- Steps are being taken to minimise disruption to operations
- Services will be restored as quickly and safely as possible
- Appropriate safeguards are in place to protect confidential information and organisational data

Where relevant, communications may also confirm that contingency arrangements support continuity of services delivered through TECI operations and subcontracted delivery partners.

21.5 Topics Staff Should Not Comment On

Staff must not speculate or provide information on the following (this list is not exhaustive):

- The number or identity of injured individuals or casualties
- The extent of damage to buildings or infrastructure
- Financial implications or estimated costs of the incident
- Possible causes of the incident or responsibility for it
- Any criticism of emergency services, partners, or other organisations involved

All enquiries from journalists or external media should be referred directly to the designated SLT spokesperson.

22. Staff Whereabouts Log

(Make one copy for each team member and update daily)

Name: **Address:**		**Telephone:** **Mobile:**
Week commencing:		
Day	AM	PM
Monday	Location: Telephone: Email:	Location: Telephone: Email:
Tuesday	Location: Telephone: Email:	Location: Telephone: Email:
Wednesday	Location: Telephone: Email:	Location: Telephone: Email:
Thursday	Location: Telephone: Email:	Location: Telephone: Email:
Friday	Location: Telephone: Email:	Location: Telephone: Email:
Saturday	Location: Telephone: Email:	Location: Telephone: Email:
Sunday	Location: Telephone: Email:	Location: Telephone: Email:

23. Recovery Site rational

National delivery will result in local BCDR plans. Local plans to also contain secondary sites/alternative support locations for all participants and ensure contractual service standards can be maintained as appropriate.

24. Summary of Work area requirements in secondary sites.

Group	Desk/Chair/Phone/PC (Cumulative)				
	1 day	3 days	5 days	2 wks.	>4 wks.
SLT		1	1	1	1
IMT		1	1	1	1
IT	1	3	2	1	1
HR		1	1	1	1
Communications	1	1	1	1	1
Finance		3	5	5	5
Repairs		3	5	5	5
Total	2	13	16	16	16

25. Key Contact Details

Surname	First Name	Department	Home Telephone Number
Fox	Jacqui	Director, Strategic Partnerships	07740 540079
Fox	Caroline	CEO	07823 336424
Pacheco	Jose	Financial Controller	0208 269 5686; 07535058287
Du Toit	Morne	Director of IT	07944 877044
Sayer	Joanne	Chief People Officer (also responsible for Facilities)	07950 984660
Jackson	Debra	Managing Director – International	07591824593
Clarke	Gemma	Academic Director	+353 857593956

26. Staff with PCs at home

Staff listed below have PCs at home that can be used during an emergency situation

Name	Location/Town	PC	Remote Access	Broadband?
Caroline Fox	Lewisham	Yes	Yes	Yes
Jacqui Fox	Lewisham	Yes	Yes	Yes
Morné Du Toit	Sidcup	Yes	Yes	Yes
Sharon Major	Newcastle	Yes	Yes	Yes
Joanne Sayer	Chislehurst	Yes	Yes	Yes
Debra Jackson	Greenwich	Yes	Yes	Yes
Gemma Clarke	Dublin	Yes	Yes	Yes
Conall Gogarty	Dublin	Yes	Yes	Yes
Keshia Siniara	London	Yes	Yes	Yes
Lynsey Whitehead	Newcastle	Yes	Yes	Yes

27. Recovery Log

Date:		Page:	
Time	**Description of event**	**Response**	**Sign**

28. BCDRP Risk Assessment and Mitigation

Risk	Potential RISK	Impact	Risk Management Approach	Early warning signs	Contingency Plan
Users cannot access data – Downtime	Med	Users cannot complete day to day business due to downtime	1) Routine maintenance planned and executed 2) Regular updates to operating systems 3) Backup servers in place a) backup domain controller b) backup database server c) data backups 4) Power Outage – UPS in place	1) Routine maintenance logs 2) Planned downtime (outages) 3) Backup server downtime 4) Virus outbreak 5) User pc's not functioning	1) Switch on Backup server's 2) Replace effected machines 3) Quarantine PCs 4) Notify relevant persons
Backup Failure	Low	Company unable to provide agreed services. Complete data loss.	Ensure a routine, effective, secure and verified backup schedule and stored chronologically. 1)Three separate backup measures in place. a) Windows Shadow copies enabled b) Daily Onsite Backup c) Daily offsite backup 2) Disaster recovery plan in place	1) Backups fail to be verified for integrity.	1) Retrieve data from alternate backup

Unauthorised Data Access / Data Theft and Manipulation	Med	Confidential Customer information loss	1) Data should be securely stored and access limited to those authorised. 2) Three phase security approach to data access is in place. 3) Data is encrypted when moved between sites. 4) Computers automatically lock after a short period of inactivity. 5) Access blocked to customer data out of office hours. 6) Regular Monitoring of security logs. 7) Physical Servers stored in a secure, temperature-controlled room. 8) Intrusion detection software. 9) Antivirus, spyware and malware software installed. 10) Cyber attack	1) Security Breach identified by network monitoring application 2) Virus / Malware / Spyware outbreak logs 3) Firewall Logs 4) MIS – Data output incorrect	1) Notify relevant persons / authorities 2) Review and assess security policies 3) Verify integrity of data and restore from backup's if necessary
User deletes data accidently	High	Employee cannot work or has deleted potential confidential customer information.	Three types of backups in place. a) Daily Data Backup on-site b) Daily Off-site Data Backup c) Windows Shadow Copies enabled (for immediate data recovery in case of accidental loss)	n/a	1) Restore from backup 2) Reassess and train users

EMAIL - Virus attacks, phishing attacks, spam	High	Damage to applications, operating systems, data, disruption of service and loss of time.	1) Raising awareness among end users on potential threats, not to open unknown attachments, user of antivirus software, prevent use of email application software using administrative credentials. 2) Install antivirus / malware / spyware software to run on-access scanning to prevent possible infection. 3) Updated security patches and updates installed on software.	1) Large amount of spam emails 2) Memory related errors 3) Abnormal behaviour reported from the end user computer 4) User reports antivirus warnings	1) Notify everyone 2) Freeze outgoing email 3) Quarantine infected machines and mailboxes 4) perform clean up
WEB BROWSER - Remote code execution, memory corruption, spoofing, execution of harmful scripts	High	The vulnerabilities can lead to corruption of memory; stop the browser from functioning and phishing.	1) Raising awareness among end users on potential threats, not to open unknown webpages. 2) Install antivirus / malware / spyware software to run on-access scanning to prevent possible infection. 3) Updated security patches and updates installed on software. 4) Firewall website access control policy and predefined policies to limit the potential of end users visiting. a) potentially unproductive websites b) potentially harmful websites	Unplanned and sudden shutdown of browsers	1) Update to the latest firewall virus and attack definition files 2) Quarantine infected machines 3) Perform clean up

External Hacking	High	Denial of Service Attack Data Theft	1) Firewall logs in place 2) Firewall polices to restrict compromises 3) Alerts on potential external security breaches	1) Logs 2) Suspicious activity logs 3) Monitor Firewall performance	1) Notify relevant persons / authorities 2) Disconnect sessions 3) Restart firewall
Man in Middle Attack	High	Data Theft	Three phase encryptions	1) Data Loss 2) Suspicious activity on firewall 3) Fluctuated connectivity	1) Notify relevant persons / authorities onnection using different encryption algorithmon using different encryption algorithm
Physical Security breach	Med	Theft of equipment Theft of data	1) Alarm System 2) Physical security measures in place 3) Comms room further secured 4) Users' ability to store access data locally not permitted all data must be stored on the central server	1) Triggered Alarm 2) Suspicious behaviour 3) Notification from others	1) Notify relevant persons / authorities 2) Rebuild systems from offsite backups
Loss of sub-contractor	Med	Supply chain breaks down, reduction in delivery	1/ Service Level Agreements are in place 2/ Strong performance management and quality teams in place to ensure risk is identified early and acted upon	1) Performance poor 2) Relationship breaks down	1/ Ops Director notifies managers monthly 2) Redirect bus to other partners 3)

29. Centre Annexes

29.1 Southwark

Overview

Centre staff are briefed to recognise situations that may contain hazards such as fire, electricity, crushing, chemical danger, social danger and other threats to personal safety. If a staff member suspects a hazard has developed / is developing / has a potential to develop, they are obliged to inform the Local Manager of the situation. If the local manager is unavailable, inform (in priority order) the Area Manager, Operations Director or Regional Director.

Emergency Response Controller

Once management ownership of the incident has been established, the nominated person becomes the ERC. Their primary duties are to:

1) Ensure the safety of all parties on site and inform emergency services / building management as needed.
2) Execute the safe relocation of staff to the nominated second site, and safe exit or redirection of other stakeholders.
3) Inform the Head Office Senior Team and take reasonable steps to safeguard the customer data stored on site via relevant authorities if there is a risk to personal safety.

Senior Team

Responsibility for the incident then transfers to SLT at per the HQ site plan. This ensures that financial and logistic assistance can be provided immediately.

Site Specific Considerations

There is no electronic data stored on site as Twin operate remote desktop and support the use of the Prime Systems for delivered contracts which are also remote. Local computers are not used for data storage and should not be prioritised in an emergency.

The Clear Desk Policy ensures that minimal customer hard copy data is exposed at any one time. Beyond staff and stakeholder safety, customer data should be locked away if possible, or that which is exposed; transported in line with the Security Policy requirements.

The nominated second site for Southwark is the Greenwich HQ site. If it is decided by SLT that some operations can continue on site, rapid contact is to be made with all customers to inform them of the issue and redirect / rebook appointments as directed by the local manager or next operational representative.

Southwark: Key Info
224-236 Walworth Road, Manor House, SE17 1JE
Tel: +442082692524
Area Manager: Parul Ahmed
Local Manager: Honey Teslim
Key Holders: Judith Bryan, Honey Teslim
Stakeholders: Ingeus, Forward Trust, Shaw Trust, JCP, DWP
Activity: National Careers Service (Shaw Trust), Restart (Ingeus), Southwark Works NEETs

29.2 Eastbourne

Overview
Centre staff are briefed to recognise situations that may contain hazards such as fire, electricity, crushing, chemical danger, social danger and other threats to personal safety. If a staff member suspects a hazard has developed / is developing / has a potential to develop, they are obliged to inform the Local Manager of the situation. If the local manager is unavailable, inform (in priority order) the Area Manager, Operations Director or Head of Assurance.

Emergency Response Controller
Once management ownership of the incident has been established, the nominated person becomes the ERC. Their primary duties are to:

1) Ensure the safety of all parties on site and inform emergency services / building management as needed.
2) Execute the safe relocation of staff to the nominated second site, and safe exit or redirection of other stakeholders.
3) Inform the Head Office Senior Team and take reasonable steps to safeguard the customer data stored on site via relevant authorities if there is a risk to personal safety.

Senior Team
Responsibility for the incident then transfers to SLT as per the HQ site plan. This ensures that financial and logistic assistance can be provided immediately.

Site Specific Considerations
There is no electronic data stored on site as Twin operate remote desktop and support the use of the Prime Systems for delivered contracts which are also remote. Local computers are not used for data storage and should not be prioritised in an emergency.

The Clear Desk Policy ensures that minimal customer hard copy data is exposed at any one time. Considered after staff and stakeholder safety, customer data should be locked away if possible, or that which is exposed be transported in line with the Security Policy requirements. Staff from external companies in a site share environment are not under contract to provide services to Twin, have not undergone our security checks and must be treated as 3rd party / members of the public in regard to security.

The nominated second site for Eastbourne is the LCT site. Once connectivity re-established, or it is decided by SLT that some operations can continue on site, rapid contact is to be made with all customers to inform them of the issue and redirect / rebook appointments as directed by the local manager or next operational representative.

Twin Employment & Training Eastbourne: Key Info
Compton Park, Compton Place Road, Eastbourne, BN21 1EH
Tel: +44 (0)1323 725 887
Area Manager: Kevin Simpson
Local Manager: Kevin Simpson
Key Holders: Kevin Simpson
Stakeholders: Staff, Customers, Partner Agencies
Activity: Multi-Purpose Employment and Skills delivery

29.3 Leicester

Overview
Centre staff are briefed to recognise situations that may contain hazards such as fire, electricity, crushing, chemical danger, social danger and other threats to personal safety. If a staff member suspects a hazard has developed / is developing / has a potential to develop, they are obliged to inform the Local Manager of the situation. If the local manager is unavailable, inform (in priority order) the Operations Director, Financial Controller, HR Manager or Head of Assurance who are based on the site; and immediately give coordination to the SLT (Emergency Team)

Emergency Response Controller
Once management ownership of the incident has been established, The SLT lead will:

1. Ensure the safety of all parties on site and inform emergency services / building management as needed.
2. Execute the safe relocation of staff to the nominated second site, and safe exit or redirection of other stakeholders.
3. Take reasonable steps to safeguard the customer data stored on site via relevant authorities if there is a risk to personal safety

Site Specific
The infrastructure and subsequent considerations are managed elsewhere in the main BCP document; and include safeguarding the assets. The nominated second site for Leicester is currently being identified. Once connectivity is re-established, or it is decided by SLT that some operations can continue on site, rapid contact is to be made with all customers to inform them of the issue and redirect / rebook appointments as directed by the local manager or next operational representative.

Stakeholders to be contacted: Later the same day:
Any invited customer or guest with a later appointment in the next 48 hours. Any staff not at the office that day. Details are to be given of alternative venues and appointment slots where possible. Where this is not possible (the immediate customers) a call back is to be arranged to provide updated information when available.

Note: System support included in contact list as CDG login is IP dependent and your ability to contact clients may be limited

Twin Employment & Training: Key Info
2nd Floor, 60 Charles Street, LE1 1FB
Tel: +44 (0)11 6502 0487 / 07805 683 622
Area Manager: Parul Ahmed
Local Manager: Parul Ahmed
Kay Holder: Parul Ahmed
Stakeholders: Staff, Customers, Partner Agencies
Activity: Multi-Purpose Employment and Skills delivery

29.4 Dublin Ireland

Overview
Centre staff are briefed to recognise situations that may contain hazards such as fire, electricity, crushing, chemical danger, social danger and other threats to personal safety. If a staff member suspects a hazard has developed / is developing / has a potential to develop, they are obliged to inform the Centre Manager in each location of the situation. If the centre manager is unavailable, inform the Academic Director or who is based on the site; and immediately give coordination to the SLT (Emergency Team)

Once management ownership of the incident has been established, The SLT lead will:

1. Ensure the safety of all parties on site and inform emergency services / building management as needed.
2. Execute the safe relocation of staff to the nominated second site, and safe exit or redirection of other stakeholders.
3. Take reasonable steps to safeguard the customer data stored on site via relevant authorities if there is a risk to personal safety
4. Centre manager or designated officer (under SLT oversight) to contact the Immediately required people list.

Site Specific:
The infrastructure and subsequent considerations are managed elsewhere in the main BCDRP document; and include safeguarding the school's assets. Once connectivity re-established, or it is decided by SLT that some operations can continue on site, rapid contact is to be made with all students to inform them of the issue and advise of re-opening date as directed by the centre manager or next operational representative.

Any staff not at the office that day. Details are to be given of alternative venues and classroom slots where possible. Where this is not possible (the immediate students) may well be taught online / another location until further notice.

Twin English Centre Ireland: Key Info: Dublin - 4 North Great George's Street, Dublin 1 DO1 A8N4 & 31 Gardiner Place, Dublin 1 DO1 EY47
Tel: +353 83 417 8393
Area Manager: Conall Gogarty
Local Manager: Conal Gogarty
Key Holders: Conal Gogarty
Stakeholders: Staff, Teachers, Students, Partner Agencies
Activity: English school.

29.5 Greenwich

Overview
Centre staff are briefed to recognise situations that may contain hazards such as fire, electricity, crushing, chemical danger, social danger and other threats to personal safety. If a staff member suspects a hazard has developed / is developing / has a potential to develop, they are obliged to inform the Local Manager of the situation. If the local manager is unavailable, inform (in priority order) the Area Manager, Operations Director or Regional Director.

Emergency Response Controller
Once management ownership of the incident has been established, the nominated person becomes the ERC. Their primary duties are to:

1) Ensure the safety of all parties on site and inform emergency services / building management as needed.
2) Execute the safe relocation of staff to the nominated second site, and safe exit or redirection of other stakeholders.
3) Inform the Head Office Senior Team and take reasonable steps to safeguard the customer data stored on site via relevant authorities if there is a risk to personal safety.

Senior Team
Responsibility for the incident then transfers to SLT at per the HQ site plan. This ensures that financial and logistic assistance can be provided immediately.

Site Specific Considerations
There is no electronic data stored on site as Twin operate remote desktop and support the use of the Prime Systems for delivered contracts which are also remote. Local computers are not used for data storage and should not be prioritised in an emergency.

The Clear Desk Policy ensures that minimal customer hard copy data is exposed at any one time. Beyond staff and stakeholder safety, customer data should be locked away if possible, or that which is exposed; transported in line with the Security Policy requirements.

The nominated second site for Southwark is the Greenwich HQ site.

Once connectivity is re-established, or it is decided by SLT that some operations can continue on site, rapid contact is to be made with all customers to inform them of the issue and redirect / rebook appointments as directed by the local manager or next operational representative.

Twin Employment & Training Greenwich: Key Info - 2 Lambarde Square, The Greenwich Centre, Greenwich London, SE10 9GB
Tel: 020 8269 5680 / +44 (0) 7969 010 586
Area Manager: Joanne Sayer
Local Manager: Joanne Sayer
Key Holders: Joanne Sayer
Stakeholders: Staff, Customers, Partner Agencies
Activity: Multi-Purpose Employment and Skills delivery