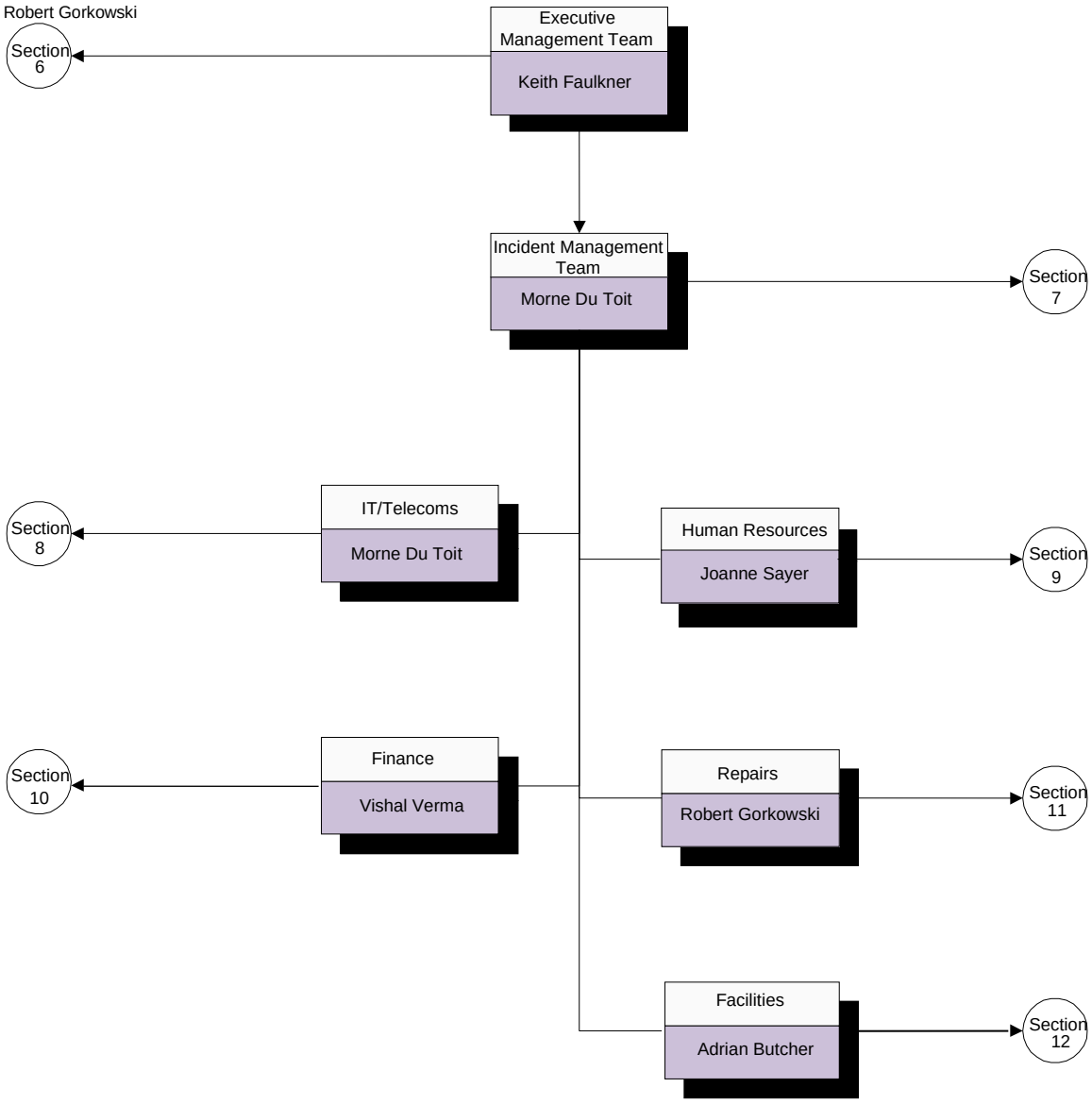
Section 1 - Contents

Contents

Originator: HR
Department: Quality Team
Version: 7.4/Aug 2022
Next Review: Aug 2023

Section 2 - Overview



Section 3 – Document Ownership/Distribution

Document owner
This document is owned by, and the Master Copy held by Joanne Sayer, Director - International Division, Operations and HR.

Distribution list
The following people have received a copy of the plan:

Copy	Name	Job Title/Department	Signed	Date
Y	Joanne Sayer	Director - International Division, Operations and HR		
Y	Caroline Fox	Chief Executive Officer		
Y	Jacqui Fox	Director, Strategic Partnerships		
Y	Keith Faulkner	Chairman		
Y	Vishal Verma	Chief Financial Officer		
Y	Sarah Morse	Executive Head		
Y	Adrian Butcher	Group Policy & Partnerships Director, TTI, Facilities Manager		
Y	Morné Du Toit	Head of IT		
Y	Debra Jackson	Chief Operating Officer		
Y	Deep Khanna	Director of Operations - Employability		
Y	Beth O' Shea	Ireland Director		

Section 3 – Document Ownership/Distribution

Revision record
The following are the recent changes that have been made to the document:

Date	Description	Author
12/06/2017	Complete Management Team update & site updates	Deep Khanna
31/01/2020	Complete Management Team update & site updates	Amanda Brade
31/01/2021	Update Management Team changes & site updates	Amanda Brade
25/01/2022	Improved formatting and added further annexes	Mark Williams

Redactions in this version:
- None relevant centre specific annexes.

Section 4 - Overview

Introduction
This plan sets out business resumption guidelines in the event of a disaster resulting in the loss or disruption to the services or the use of Twin Group HQ Greenwich, or other Twin operational sites. We have concentrated on a worst-case scenario (for example the possibility of a major fire) as it is more practical to be fully prepared for the worst. The plan also considers other continuity issues that could affect service delivery such as a breach in IT security, the loss of a major supplier or sub-contractor, widespread illness, transport disruptions, weather disruptions, etc.

The benefits of implementing a recovery plan quickly are significant. They include:

- operational recovery
- minimised loss
- maintained service levels to meet obligations
- restored sub-contractor and stakeholder relationships
- ensure customers/ learners continue to be serviced safely and professionally

The safety of staff and customers is of the highest priority. Several factors have been identified to ensure prompt response to and limitation of damage as far as possible in the event of a catastrophe. These include:

- dealing with casualties and counselling staff and customers
- contacting staff and customers to inform them of the current position and our future plans
- relocation of the staff and based in the damaged building to an appropriate recovery site
- getting all computer and communications systems which have been identified as critical, up and running as soon as possible.

Inevitably the guidance given cannot be comprehensive and applicable to all eventualities. Flexibility will be required, depending on the nature and seriousness of the crisis, and the Incident Management Team (with the emergency authorities) will determine the approach.

The handbook will be updated regularly by Joanne Sayer and amended copies will be distributed accordingly. The head of each business unit is responsible for keeping their own sub-plan up to date and communicating any changes to Joanne Sayer. Further maintenance guidelines can be found towards the end of this document.

Anyone who is mentioned in the handbook is asked to notify Human Resources of any changes in their personal details, and Joanne Sayer in any changes in procedures or areas of responsibility as soon as they occur.

The plan contains information necessary to recover from a total loss of, or denial of, access to, our offices at: The Greenwich Centre, 12 Lambarde Square, London SE10 9GB and satellite centres.

Other Scenarios
With regard to less serious business continuity issues, that does not prevent Twin HQ from being utilised as head office but are due to a lack of staff being available, please note the following.

All HODs are responsible (and in their absence, their designated second) for informing their respective members of their teams and their manager of the nature of the issue and also for the provision of adequate back up plans to ensure business continuity until the issue is resolved. Should an entire department be unavailable, then the HODs Manager is responsible for ensuring that there is an adequate back up plan.

Section 4 - Overview

Layout of the plan
The Business Continuity Plan is a detailed overview of the recovery plans. This gives guidance to the various teams and business units who will be involved in the recovery:

- the emergency response controller: first call out procedures
- the Executive Management Team: strategic decision making and communications
- the Incident Management Team: co-ordination of the recovery response, damage assessment, salvage and insurance
- the Infrastructure Recovery Team: setting up and maintaining the recovery site, IT and communications
- the business units: continuation of key business processes, prioritised by time criticality agreed with the business

The following plans are hosted on the company intranet:

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

Recovery Strategy
If main office location Twin HQ, Greenwich is unavailable, invoke the Business Continuity plan and prepare staff and customer transport arrangements to the recovery site. Where applicable, staff will work from home and customers will be advised not to attend.

If a satellite office is not usable in the London area, staff are to refer to the Centre Annex that relates to their location for specific advice.

For sites outside of the London area, staff are to work from home where possible pending an update from their Business Unit Manager or the nominated Emergency Response lead.

Learners will be sent home with immediate effect and guardians notified.

Section 5 – Emergency Response Controller

Emergency Response Controller

Responsibilities

The emergency response controller is the first person to respond to an alert regarding a major problem at Twin sites.

During office hours the Emergency Response Controller will be the Fire Officer or their deputy. They will hand over control to the senior member of Group Executive Team (GET) present once the office has been evacuated and it has been determined that a major incident has taken place.

Outside of office hours, a keyholder will take responsibility until the most senior member of GET available has been alerted and assumed responsibility.

The key roles and responsibilities of the emergency response controller are:

- give instructions to the fire wardens
- identify danger areas to be avoided
- identify safe areas to assemble
- ensure building is evacuated
- to conduct an initial investigation to establish the severity of the incident
- decide what action to take (e.g. contact Group Executive Team)
- convene Incident Management Team if situation is serious
- notify and liaise with emergency services
- initiate evacuation procedures

Once the Incident Management Team has been convened, the role of the emergency controller ceases to exist. Responsibility for liaison with emergency services will transfer to facilities staff based at the damaged site.

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

Name	Title/Role	Contact Details
Morné Du Toit	Chief Fire Warden / Key holder / Head of IT	07772003045
Adrian Butcher	Facilities Manager	07969 010586
Robert Gorkowski	Building Manager	07920110208

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 Deep Khanna (07825781504).

Emergency response controller's requirements

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

Section 5 – Emergency Response Controller

Keyholders Instructions for Access to HQ Main office

Keyholders are issued with 3 keys to the doors of main office.

When the building manager leaves at 8.00 pm, the doors to the reception and the Rear Entrance will be locked. To gain entry you will need a key.

Satellite centres have equivalent processes that should be reviewed.

The Intruder alarm is set each weekday evening with sensors monitoring the whole of the floor areas and access doors plus the stairwells. The alarm system control box is in the reception area. It will go off if any of the sensors are tripped. To turn the alarm off you should enter the building via the front door and input your four-digit code into the control box. To enable or turn on the alarm, the procedure is the same with the addition of having to press the “Yes” button once the four-digit code is entered. This should only be done after all areas have been vacated, all doors are properly closed, and the rear door locked. After inputting your code and pressing the “Yes” key, you should exit the building immediately via the front door.

Section 6 – Group Executive Team Plan

Group Executive Team (GET) Plan

The Group Executive Team meet on an exception basis to discuss group performance ensuring a quality service provision is being supplied and that no areas detailed in this plan pose a risk to the business. Whilst this plan takes into account the worst-case scenario the GET Team recognise that there are additional risks that can affect service delivery. Any issues that are highlighted as being at risk are discussed and acted upon.

Responsibilities

To manage the business issues throughout the emergency or loss of service provision as well as providing support and direction to the Incident Management Team if required.

GET recovery objectives	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks	>4 wks
Manage strategic response	□	□	□	□	□
Liaise closely with business teams via regular meetings	□	□	□	□	□
Meet regularly with Incident Management Team	□	□	□	□	□
Take overall responsibility for staff welfare	□	□	□	□	□
Manage business relationships to ensure effective continuation of service delivery	□	□	□	□	□
Authorise expenditure of large unforeseen amounts	□	□	□	□	□
Ensure Board are aware of situation	□	□	□	□	□
Authorise decision to refurbish primary site or seek new premises				□	□

Team Location

The GET recovery site will be either:

- Lewis Grove Centre
- Southwark Centre

At the time of the incident, one member of the GET will agree which site will be used.
See Emergency Controller list (P8) for team members able to authorise relocation; in addition to the Business Owners.

Section 6 – Group Executive Team Plan

Vital records

The Executive Management Team's Recovery SharePoint Sitees will be held at The Greenwich Centre, 12 Lambarde Square London SE10 9GB and 1 Lewis Grove London SE13 6BG

Recovery SharePoint Site contents:

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

Infrastructure needs

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

Section 6 – Group Executive Team Plan

Action plan

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

Days 2-3 – Actions	Status
Hold a meeting with IMT for an update on damage assessment of primary site, 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 business partners	
Update Chairman and make remaining Board members aware	
Ensure that when staff are questioned about the incident, the message they give is appropriate	

Section 6 – Group Executive Team Plan

Days 4-5 – Actions	Status
Hold meetings with IMT and Divisional Directors for updates on the situation	
Ensure that management remains visible and accessible.	

Days 5-14 – Actions	Status
Consult with IT Recovery Team, insurers, IMT and relevant others to evaluate damage to Organisation name.	
Continue regular meetings with IMT and Operational Managers	
Continue liaison with Board	

Days 14-28 – Actions	Status
If the main site will not become habitable within one month, meet with the Infrastructure Recovery Team to plan longer-term recovery options. Otherwise, authorise reconstruction and refit of Twin Lewisham. Also investigate the availability of local office space for short-term rental.	
Continue liaison with Board	
Liaise with the IMT and Operational Managers to develop a long-term recovery strategy.	

Section 7 – Incident Management Team

Incident Management Team (IMT) Plan

All essential staff are identified by the IMT, and other staff members are trained to take over their roles or responsibilities in emergency situations. This process will be implemented throughout the supply chain incorporating existing processes that the delivery partners already undertake. All key departments within the supply chain including finance, IT and GET Team, are not reliant upon one individual and so teams can remain fully functional in the absence of the Manager of that team.

In the event of an IT security breach all employees are to contact their manager and the IT Manager. There is a two-hour response policy during office hours and a six-hour response policy at all other times to deal with serious incidents, such as virus infections. In addition, the IT Administrator will monitor the server and firewall regularly to make sure that there is no suspicious activity taking place, with the Head of IT taking overall responsibility. Further details about the process communicated to staff about the IMT process can be found in the IT Security Plan on the intranet.

Responsibilities

To manage and co-ordinate the activities associated with the invocation of the Business Continuity Plan.

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

Team Location
The IMT recovery site will be either:

- The Greenwich Centre, Greenwich London SE10 9GB
- Lewis Grove Centre, Lewisham London SE13 6BG
- Or all are home based if the above sites are required for other activities in the business

At the time of the incident, one member of the Incident Management Team will agree which site will be used.

Section 7 – Incident Management Team

Team Members

Name	Department / Title	Function	Contact details
Joanne Sayer	Group Operations Director	Leader	
Vishal Verma	Chief Financial officer	Team Member	
Morné Du Toit	Head of IT	Team Member	
Adrian Butcher		Team Member	
Jacqui Fox		Team Member	

Vital records

The Incident Management Team's Recovery SharePoint Sitees will be held at The Greenwich Centre, 12 Lambarde Square, Greenwich SE10 9GB & 1 Lewis Grove, Lewisham, London SE13 6BG.

Recovery Sharepoint Site contents:

Recovery item	Status
DR IT recovery invocation procedures	
Managers contact list	
Supplier contact list	
Pre-prepared statements and list of recipients	
Contact name and number for insurance broker	

Infrastructure needs

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

Section 7 – Incident Management Team

Action plan

Day 1 – Actions	Status
Initiate recovery log. Record all activity relating to the recovery.	
Contact GET leader, brief on current position and agree initial strategy. Agree on timings of next updates.	
Obtain GET 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 GET 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 GET.	
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.	
Inform insurers of the situation and arrange a visit of the loss adjusters.	

Section 7 – Incident Management Team

Days 2-3 – Actions	Status
Engage salvage company and structural engineers to provide an assessment of the damage. Provide floorplans.	
Hold status update meetings with other recovery teams and communicate status to GET	
Hold status update meetings with other recovery teams and communicate status to GET	
Confirm that IT and business operations at the recovery site are established	
Continue liaison with emergency services, GET, ITTRT and insurance company	
Receive any unexpected business visitors at the co-ordination centre and advise them of new business contact arrangements.	
Provide staff at the recovery site with approved statements to respond to incoming enquiries	

Days 4-5 – Actions	Status
Arrange a meeting to establish insurance and reconstruction responsibilities	
Agree purchasing and budgetary limits with insurers. Authorise placement of orders/ invocation or emergency procurement agreements for equipment	
Continue liaison with emergency services, GET, 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 GET	
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 time-scales, 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	
Continue liaison with emergency services, GET, ITTRT, insurance company and Divisional Directors	

Section 8 – IT Recovery Plan

IT Recovery Team Plan

Twin's telecoms is hosted by MS Teams so no recovery process required

Majority of systems are hosted in the cloud so will go unaffected by losses of physical locations. A handful of systems do remain onsite in Greenwich - Sage 50, PO DB, GT DB
Twin's servers are backed up every day and kept secure on the premises and offsite, along with copies of all software and database software. All IT staff are trained to enable Twin to re-instate systems very rapidly.

Responsibilities

To provide appropriate resources to ensure a safe, secure and efficient business recovery environment including premises and IT.

Infrastructure recovery objectives	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks	>4 wks
Liaise with Incident Management Team (IMT) and Group Executive Team (GET)	☐	☐	☐	☐	☐
Prepare recovery site according to priority of business functions as defined by GET	☐	☐	☐	☐	☐
Retrieve off site resources	☐	☐	☐		
Telecommunications redirection	None				
Reconstruct IT and Telecommunications requirements at recovery site	☐	☐	☐	☐	☐
Reconstruct critical premises requirements at recovery site	☐	☐	☐	☐	☐
Reconstruct support services at recovery site	☐	☐	☐	☐	☐
Liaise with DR IT and equipment suppliers	☐	☐	☐	☐	☐
Ensure business recovery staff are aware of support arrangements	☐	☐	☐	☐	☐
Ensure temporary IT recovery resources are secure overnight – security guard required?		☐	☐	☐	☐
Assist with damage assessment	☐	☐	☐		
Maintain and update web site for customer information	☐	☐	☐	☐	☐

Team Location
The ITTRT recovery site will be:

- Lewis Grove, Lewisham

At the time of the incident, one member of the IT Management Team will agree which site will be used.

Section 8 – IT Recovery Plan

Team Members

Name	*Department / Title*	*Function*	*Contact details*
Morné Du Toit	Head of IT	Deputy Leader Hardware and Software Rebuild	077 7200 3045
Otis Kotsanos	IT Administrator	Users' setup	07798836167

Vital records
The Infrastructure Recovery Team's Recovery SharePoint Site

Recovery Sharepoint Site contents:

Recovery item	Status
IT Disaster Recovery Plan (server build documentation, workstation build documentation, network diagram).	
Key contact lists (suppliers, sub-contractors, key stakeholders)	
System passwords	
List of staff authorised to invoke DR recovery contract	
DR IT invocation procedure	
DR IT recovery centre location maps	
Asset list	

Section 8 – IT/Telecommunications Recovery Plan

System needs

Group	Quantity/timeframes				
	1 day	3 days	5 days	2 wks	>4 wks
GET		1	1	1	1
IMT		1	1	1	1
IT		3	2	1	1
HR					
Communications					
Finance		3	5	5	5
Repairs		3	5	5	5
Total	0	13	16	15	15

Section 8 – IT Recovery Plan

Action plan

Day 1 - Actions	Status
Agree time for initial meeting	
Retrieve Recovery SharePoint Site	
Divert telecoms systems to Eastbourne and update messages	
Retrieve backup media from Lewis Grove centre	
Gain authorisation from GET and invoke recovery from suppliers. Confirm estimated time of arrival, availability of recovery facility and numbers of attendees	
Gain authorisation from GET and invoke business continuity plan. Inform sub-contractors of situation and gain estimate of recovery timings	
Arrange redirection of trunk lines to recovery site and ensure appropriate message is in place for incoming calls	
Set up remote access for all staff with remote access at home	
Investigate shuttle bus arrangements for staff transport to recovery site	
Provide GET, IMT and operational managers with estimated time of recovery of each service	
Advise IMT of progress	
Ensure recovery staff are aware of support arrangements	

Days 2-14 - Actions	Status
As soon as possible, begin server recovery	
Provide IT support services at recovery site	
Reconstruct non-standard PCs	
Assist as required with salvage operation	
Perform system checks	
Maintain backup offsite procedures	
Rebuild switch at recovery site as soon as access is possible. Link numbers to handsets using a list of staff expected to attend the recovery site, plus their job descriptions	
Decide whether to continue inputting as normal	

Section 8 – IT Recovery Plan

Days 2-14 - Actions	Status
Decide whether to continue inputting as normal (dependent upon decision to continue processing new business)	
Manage staff at recovery site and salvage team at damaged premises	
Advise all essential contacts, including sub-contractors of situation and new contact details	
Review equipment installed at the recovery site	
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	

Systems restoration

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

Days 14-28 - Actions	Status
Continue as Days 2-14	
Begin to prepare for return home. Inspect site, review salvaged equipment, agree purchasing requirements, produce project plan	

Section 9 – HR Recovery Plan

HR Team Recovery Plan

Responsibilities

To manage and co-ordinate the activities associated with HR aspects of the Business Continuity Plan. To ensure the payroll function can be re-established and that staff issues (expenses, welfare, counselling etc.) are resolved appropriately during the incident.

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	□	□	□	□	□
Regular contact with non-recovery staff	□	□	□	□	□
Activate counselling where appropriate	□	□	□	□	□
Provide regular briefings for all staff about expenses / payments / welfare		□	□	□	□
Maintain contact with finance team and submit payroll information for processing		□	□	□	□
Maintain confidentiality of personnel records	□	□	□	□	□
Liaise with Incident Management Team and Emergency Management Teams	□	□	□	□	□

Team Location

At the time of the incident, the HR Management Team will agree a temporary site near to HQ. The location will be the Lewis Grove, Lewisham, SE13 6BG.

Name	Department / Title	Function	Contact details
Joanne Sayer	Director - International Division, Operations and HR	Staff Management	07950984660
Andrew Tsui	HR Manager	Staff Management	
Jacqui Fox	Director, Strategic Partnerships	Staff Management	07740540079
Vishal Verma	Chief Financial Officer	Staff Management	

Section 9 – HR Recovery Plan

Vital records

The HR Team's records are stored electronically on People HR. Recovery SharePoint Sitees will be held at Lewis Grove, Lewisham.

Recovery SharePoint Site contents:

Recovery item	Status
Staff list with address and contact and 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	

Infrastructure needs

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

Systems requirements

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

Section 9 – HR Recovery Plan

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	
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)	

Section 9 – HR Recovery Plan

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 staffing needs and recruitment processes	

Section 10 – Finance Recovery Plan

Finance Team Recovery Plan

All accounting and financial data is either on Sage, Class or the Twin server. All these data is backed up by IT and is covered in IT recovery plan.

As the accounting records are paperless there should be no loss except any documents/ letters received in the last week or so if these haven't been scanned. All statutory and permanent information is archived safely but again there are soft copies on the server in case of theft or fire.

Responsibilities

To manage and co-ordinate the activities associated with Finance aspects of the Business Continuity Plan and support the business to navigate through any crisis.

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

Team Location

At the time of the incident, the Finance Management Team will agree a temporary site near to Greenwich HQ. The initial location for the team will be the Lewis Grove Centre in Lewisham or the team will work remotely from their respective homes.

.

Name	Department / Title	Function	Contact details
Vishal Verma	Chief Financial Officer	Leader	07950668146
Jose Pacheco	Group Finance Controller	Deputy Leader	0208 269 5686; 07535058287

Stuart Harris	Finance Analyst	Deputy Leader Payments & Credit Control (TET)	0208 269 5673
Deirdre Lensley	Accounts Assistant	Accounts Payables	0208 269 7533

Vital records

The Finance Team's Recovery SharePoint Site will be held electronically and temporarily set at Lewis Grove, Lewisham, SE13 6BG.

Section 10 – Finance Recovery Plan

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	

Infrastructure needs

A safe for storing petty cash, plus:

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

Systems requirements

System	Timeframes				
	1 day	3 days	5 days	2 wks	>4 wks
Sage System		2	3	3	3
Access to all Government related systems such as TTS, Bravo, e-Claims		2	3	3	3
PICs/Class/CRM		1	2	2	2
e-mail and Microsoft Office		2	5	5	5
Bank Account Access	2	2	2	3	3
Access to the server		5	5	5	5

Section 10 – Finance Recovery Plan

Action plan

Day 1 – Actions	Status
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 Finance team leaders to confirm 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 Group Executive Team (GET). Relocate recovery team to short term location.	
Hold initial planning meeting. Make contact with Group Executive Team (GET) and report immediate status. Agree time and venue of next meeting.	
Advise essential contacts of situation and contact details.	
Obtain confirmation from GET 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 GET 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	

Days 2-3 – Actions	Status
Evaluate the effect of any lost transactions on business operations	
Continue regular communication with GET. 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	
Relocate cash receipts to recovery site.	

Section 10 – Finance Recovery Plan

Days 4-5 – Actions	Status
Relocate Management Accounts recovery representative to the recovery site and commence production of reports or reconstruction of financial records	
Continue Banking and Payments activity as Days 1,2-3.	
Continue regular communication with GET.	
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.	

Section 11 – Facilities Recovery Plan

Facilities Team Recovery Plan

Responsibilities

To provide appropriate resources to ensure a safe, secure and efficient business recovery environment.

Facilities recovery objectives	Timeframes (Approx.)				
	1 day	3 days	5 days	2 wks	>4 wks
Liaise with Incident Management Team (IMT) and Group Executive Team (GET)	☐	☐	☐	☐	☐
Prepare recovery site according to priority of business functions as defined by GET	☐	☐	☐	☐	☐
Reconstruct support services at recovery site	☐	☐	☐	☐	☐
Ensure business recovery staff are aware of support arrangements	☐	☐	☐	☐	☐
Ensure temporary recovery resources are secure overnight – security guard required?		☐	☐	☐	☐
Assist with damage assessment	☐	☐	☐		

Team Location

At the time of the incident, the Facilities Management Team will agree a temporary site near to Twin HQ, Lewisham. The initial location for the team will be Lewis Grove, Lewisham.

Name	Department / Title	Function	Contact details
Adrian Butcher	Facilities Management	Office Infrastructure Management	07969 010586

Vital records

The Facilities Team's Recovery SharePoint Site will be held at Lewis Grove, Lewisham, SE13 6BG, 12 Lambarde Square SE10 9GB and electronically at (link)

Recovery SharePoint Site contents:

Recovery item	Status
Supplier 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	

Infrastructure needs

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

Section 11 – Facilities Recovery Plan Template

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	

Section 12 – Plan Review and Maintenance

Plan Review and Maintenance

Updating the Plan

This section explains the procedures for updating Twin Groups Business Continuity Plan. Updating the Plan with revised recovery procedures is the responsibility of each Business Recovery Team Leader.

A structure is in place to: -

- Authorise any removal and updating of recovery procedures held in any of the distributed Business Continuity Plans.
- Keep a record of all updates made to the Business Continuity Plans so that the Plan is sure to be the most recent version.
- Conduct regular audits of the distributed plans to ensure version integrity.

It is the responsibility of all team members to ensure that any changes to data contained within this plan, e.g., to preferred suppliers, sub-contractors or contact telephone numbers should be notified to the team leader.

On a regular basis the following should take place:

- A run through involving as many members as possible, including managers should be arranged to identify and changes in working practices since the plan was last reviewed.
- Check that only current versions of the plan are in use
- Update 'open issues' sections and communicate to the relevant groups or individuals.

Distribution

An up-to-date copy of the Business Continuity plan is held:

- Electronic version to held on Twin Group on Ms Teams
- Each individual mentioned in this document must have access to the plan, showing the date and version number of the last update

The distribution list is checked monthly, to ensure that relevant personnel hold a copy, and that copies are retrieved from staff who leave the group.

Version numbering / dates

A version number or date appears on each page of the plan document. Each time the plan (or part of the plan) is amended and distributed; the old version must be destroyed by the same methods used for confidential documents. Signoff must be gained from each Recovery Team Leader to ensure that their part of the plan has been reviewed and is considered up to date.

Update schedule

The disaster recovery plan should be updated:

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

Section 12 – Plan Review and Maintenance

Category	Rec. Update frequency	Update responsibility	Last updated Name	Date
Review business risks	6 monthly	GET	Joanne Sayer	
Review impact analysis	6 monthly	GET	Joanne Sayer	
Review critical IT systems	3 monthly	GET/IT Manager	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	Joe Sayer	
External contacts	3 monthly	GET/ Function Managers	Vishal Verma	
Recovery requirements	6 monthly	GET	Joanne Sayer	
Recovery location details	6 monthly	Head of IT	Morné Du Toit	
Any other details likely to change regularly	3 monthly	Operational Managers/Head of IT	Joanne Sayer/Morné Du Toit	

When changes are made to the plan, any other groups who may be affected (e.g., IT) will be informed.

Minimum update frequency for all tasks is annually or upon a critical incident or milestone that alters the topic in question.

Section 12 – Plan Review and Maintenance

Maintenance Lists

Executive 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	

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.	
Keep details of external personnel/organisations able to assist with expert services at the time of an emergency.	

Section 12 – Plan Review and Maintenance

IT Team

Activity	Box
Be aware of local property availability and, if appropriate, re-evaluate recovery strategy based on findings.	
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.	
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.	

Section 12 – Plan Review and Maintenance

Business Functions

Activity	Box
Understand the impact to the Company of the business activities being out of action.	
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.	
Develop and maintain the Business Team's own plan unit.	

Section 13 – Testing Guidelines

Testing

Introduction

Testing is essential in providing confidence that the objectives of the Plan can be achieved. It also provides an ideal training opportunity for those involved in the key activities. All testing must be carefully managed and co-ordinated to ensure low risk to the business but with maximum return on the effort put in. This section described the different methods by which Twin Group Business Continuity Plan can and will be tested.

Description	Objective	Test frequency	Last test
IT test at recovery site	• To ensure all critical IT systems can be recovered. • To advise management of timescales for critical systems to be recovered.	6 monthly	Nov 2021
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	6 monthly	Nov 2021
IT recovery and recovery teams at recovery site	• Simulate 'real' disaster situation including penetration tests to pull all teams together.	Yearly	Nov 2021

Section 14 – Sample Media Statements

Media statement

An emergency press statement in the event of a major incident impacting on main office site should only be issued by [name of individual] (or another member of GET determined by GET at the time) in the event of being door-stepped by the press.

[Name of company]

As a result of a nearby [*gas explosion/bomb threat*] within the vicinity of Main office site, the premises of Twin Group 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 Group 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 Group 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 Group 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.

It is our intention to liaise closely with 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.

Additional information

The overriding tone should be one of co-operation (i.e. "I am not being unhelpful, I just don't know any more at this stage, but we will give you a Twin Group contact number as soon as we can."). It is easy and acceptable, at an early stage of a crisis to say "I'm sorry I do not have any information on that, you had better ask the police", or as many variations on this as you can think of.

Q & A's

1. What was the cause of the gas leak and when did you first hear about it?

The cause has not yet been identified but British Gas is undertaking a thorough investigation to ensure the source is found and that there is no longer any threat to people's safety. Twin Group was notified instantly of the situation and as a result put its well-rehearsed procedure into place. The premises were successfully evacuated within 5 minutes.

Section 14 – Sample Media Statements

2. Who was behind the bomb threat?

Twin Group does not wish to comment on this matter. Such questions will need to be referred to the emergency services. We simply followed all procedures in response to the bomb threat and are now concentrating on resuming business within the next 24 hours.

3. You seem confident that you can be up and running very quickly. Were you expecting this to happen?

There is no way that we could foresee such an occurrence but Twin Group prides itself on its professionalism and this is reflected in the way that we have a business continuity plan in place. We acknowledge the importance of planning for any eventuality and that our customers need to be safe in the knowledge that their affairs are in safe hands. Meticulous planning is just one way in which Twin Group looks to protect both itself and those people associated with us.

4. Can you be absolutely certain that customers will not be affected by this unfortunate incident?

As you can appreciate, when a company has to temporarily close down its offices and all of the systems within it, there is a huge level of immediate activity. The priority has to be to ensure that everyone is evacuated safely from the building and then making sure every effort is made to limit the damage caused.

Twin Group always backs up its system so in the event of our offices being closed, all customer transactions continue as per normal.

5. Were there any casualties?

There were no casualties and the way in which people remained calm and orderly always was no doubt a reason behind this. The emergency services are now taking further action in making sure the area is safe for everyone to return to work.

or

I am saddened to say that there are initial reports of minor casualties (significant casualties etc) as a result of the explosion that took place in main office site.) I am unable to release exact details as the emergency services are on the scene evaluating the current situation. As soon as we have more information, it will be relayed to you straight away.

Our first concern now is to help those people injured and ensure that there is no further risk to people's safety.

Section 14 – Sample Media Statements

Media handling guidelines

Messages to bear in mind
• the police are dealing with all casualties • the firm is not at present in a position to comment on, or evaluate, the position in any detail • reassuring messages to family and friends that anyone who required medical attention or assistance is being looked after • the firm has planned for such an event and confirmation that the firm's recovery procedures are in operation and working effectively • a general message to our clients, that despite some disruption, the firm is getting on with recovering the business and we expect it will be "business as usual" from our premises as soon as possible • the firm's clients have nothing to worry about as all necessary precautions have been taken to ensure confidential information has been recovered and is secure. **Don't comment on** • the number of dead or injured • extent of damage • estimate of potential cost • theories as to what happened or those responsible • any criticism of those responsible.

Section 15 – Staff Whereabouts Log

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: Fax:	Location: Telephone: Fax:
Tuesday	Location: Telephone: Fax:	Location: Telephone: Fax:
Wednesday	Location: Telephone: Fax:	Location: Telephone: Fax:
Thursday	Location: Telephone: Fax:	Location: Telephone: Fax:
Friday	Location: Telephone: Fax:	Location: Telephone: Fax:
Saturday	Location: Telephone: Fax:	Location: Telephone: Fax:
Sunday	Location: Telephone: Fax:	Location: Telephone: Fax:

Section 16 – List of Available Recovery Sites

Recovery Sites

Recovery Site	1st Pref	2nd Pref	Used By
Private Accommodation, Lewisham	Management Team	IMT Team	Delivery Team
Croydon Centre, Marco Polo House	IMT / HR Team	IT Team	Delivery Team
Lewis Grove, Lewisham	Finance Team	Admin Team	Delivery Team

Section 17 – Summary of Work Area Requirements

Summary of Work area Requirements

Group	Desk/Chair/Phone/PC (Cumulative)				
	1 day	3 days	5 days	2 wks	>4 wks
GET		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

Section 18 – Managers/Key Staff Contact Details

Surname	First Name	Department	Home Telephone Number
Fox	Jacqui	Director, Strategic Partnerships	07740 540079
Fox	Caroline	CEO	07823 336424
Verma	Vishal	Chief Financial Officer	
Du Toit	Morne	Head of IT	07944 877044
Gorkowski	Robert	Property	07920 110208
Sayer	Joanne	HR & Operations	07950 984660
Jackson	Debra	Chief Operating Officer	07591824593
O'Shea	Beth	Group Business Development Director	07837 835483
Butcher	Adrian	Group Marketing Director	07969 010586
Morse	Sarah	Executive Head of Schools	020 8269 5669
Khanna	Deep	Director of Operations - Employability	07825781504
Brade	Amanda	Head of Quality (Group)	07772 219119

Section 19 – Staff Home Laptop/ PC List

Staff with PC's 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
Adrian Butcher	London	Yes	Yes	Yes
Vishal Verma	London	Yes	Yes	Yes
Amanda Brade	Teddington	Yes	Yes	Yes
Beth O'Shea	Lewisham	Yes	Yes	Yes
Joanne Sayer	Chislehurst	Yes	Yes	Yes
Debra Jackson	Greenwich	Yes	Yes	Yes
Deep Khanna	Ruislip	Yes	Yes	Yes

Section 20 – Recovery Log

Recovery Log

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

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 pc's 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.	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 webpage's. 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 encryption	1) Data Loss 2) Suspicious activity on firewall 3) Fluctuated connectivity	1) Notify relevant persons / authorities 2) Disconnect / Reconnect the network connection 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)

Section 21 – Centre Annex: 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, Group 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 Group Executive Team and take reasonable steps to safeguard the customer data stored on site via relevant authorities if there is a risk to personal safety.

Group Executive Team
Responsibility for the incident then transfers to GET 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 is currently being identified. Once connectivity re-established, or it is decided by GET 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 Southwark Key Info
Manor House, 4th Floor, 224 - 236 Walworth Road, Southwark, London, SE17 1JE
Tel: 07739 321715
Area Manager: Darsh Ratna
Local Manager: Tola Akanmu
Key Holders: Darsh Ratna, Tola Akanmu
Stakeholders: Staff, Customers, Partner Agencies
Activity: Multi-Purpose Employment and Skills delivery

Centre Annex: 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, Group 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 Group Executive Team and take reasonable steps to safeguard the customer data stored on site via relevant authorities if there is a risk to personal safety.

Group Executive Team
Responsibility for the incident then transfers to GET 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 is currently being identified. Once connectivity re-established, or it is decided by GET 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 Pl Rd, Eastbourne, BN21 1EH
Tel: Area Manager: 01323 725887
Local Manager: Tracey Cook
Key Holders: Tracey Cook
Stakeholders: Staff, Customers, Partner Agencies
Activity: Multi-Purpose Employment and Skills delivery

Centre Annex: Lewisham

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 Group Operations Director, Financial Controller, HR Manager or Head of Assurance who based on the site; and immediately give coordination to the GET (Group Emergency Team)

Emergency Response Controller
Once management ownership of the incident has been established, The GET 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. Local manager or designated officer (under GET oversight) to contact the Immediately required people list.

Site Specific:
The infrastructure and subsequent considerations are managed elsewhere in the main BCP document; and include safeguarding the Work Programme assets. The nominated second site is currently being identified. Once connectivity re-established, or it is decided by GET 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 Lewisham: Key Info
1st Floor, 1 Lewis Grove, Lewisham, London SE13 6BG
Tel: 07969 010586
Key Holders: Adrian Butcher
Stakeholders: Staff, Customers, Partner Agencies
Activity: Multi-Purpose Employment and Skills delivery
currentlv not in use

Centre Annex: 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 Group Operations Director, Financial Controller, HR Manager or Head of Assurance who are based on the site; and immediately give coordination to the GET (Group Emergency Team)

Emergency Response Controller
Once management ownership of the incident has been established, The GET 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 is currently being identified. Once connectivity is re-established, or it is decided by GET 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 & 13th Floor, 60 Charles St, Leicester, LE1 1FB
Key Holders: Parul Ahmed
Stakeholders: Staff, Customers, Partner Agencies
Activity: Multi-Purpose Employment and Skills delivery

Centre Annex: Twin English Centre 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 (in priority order) the Operations Manager, Director, Director of Studies, Head of Operations or who is based on the site; and immediately give coordination to the GET (Group Emergency Team)

Emergency Response Controller
Once management ownership of the incident has been established, The GET 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 GET oversight) to contact the Immediately required people list.

Site Specific:
The infrastructure and subsequent considerations are managed elsewhere in the main BCP document; and include safeguarding the school's assets. The nominated second site for TECI is the Gardner Street building. Once connectivity re-established, or it is decided by GET 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.

Stakeholders to be contacted: Later the same day:
Any students or visitors due in the next 48 hours.
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 until further notice.

Twin English Centre Ireland: Key Info
4 North Great George's St, Dublin 1, ROI
Key Holders: Mick Leonard, Beth O'Shea,
Mary O'Sullivan, Bruna Martinelli
Stakeholders: Staff, Teachers, Students, Partner Agencies
Activity: English school and work experience hub.