Chesterfield College Group

Ofsted Good Provider

Business Continuity Plan

Policy Family:	Finance and Corporate Services
Reference Code:	FIN10
Issue Number:	5
Originator:	Assistant Principal Finance, IT and Estates
Responsible Manager:	Assistant Principal Finance, IT and Estates
Committee for Approval:	Finance and Corporate Services
Approval Date:	19 June 2025
Issue Date:	20 August 2025
Review Due:	2025/26

Impact Assessment Status: In preparing the Policy, any potential disproportionate impact it might have upon individuals with protected characteristics, as defined in the Equality Act 2010, have been carefully considered. It is the conclusion of the College Group that the Policy does not adversely impact on individuals with any of the protected characteristics.

Contents

Executive Summary

The Business Continuity Plan outlines how the college will continue operating during an unplanned disruption in service. It is more comprehensive than a disaster recovery plan and contains contingencies for business processes, assets, human resources, and business partners – every aspect of the business that might be affected. The Plan contains a checklist of suppliers and equipment, data backups, and backup site locations. It also identifies plan administrators and includes contact information for emergency responders, key personnel, and backup site providers. The Plan provides detailed strategies on how business operations can be maintained for both short-term and long-term outages.

A key component of the Business Continuity Plan is a disaster recovery plan that contains strategies for handling IT disruptions to networks, servers, personal computers, and mobile devices. The Plan covers how to re-establish office productivity and enterprise software so that key business needs can be met. There are three primary aspects for key applications and processes:

1. **High availability:** provide capability and processes so that the college has access to applications regardless of local failures. These failures might be in business processes, physical facilities, or IT hardware or software.

2. **Continuous operations:** safeguard the ability to keep things running during a disruption, as well as during planned outages such as scheduled backups or planned maintenance.

3. **Disaster recovery:** establish a way to recover a data centre at a different site if a disaster destroys the primary site or otherwise renders it inoperable.

Chesterfield College consists of two campuses in the town of Chesterfield which are used by the college to tutor students for different courses. The main campus is on Infirmary Road and is where most of the students learn, as well as being the administrative centre of the college. This campus has North Blocks, South Block Tower, East Block Engineering Workshops, West Block and Wharf Lane Workshops. The second campus is the Queen's Park Leisure Centre.

The college has satellite sites in Derby and Mastin Moor. These sites offer training and arrange apprenticeships.

Key stakeholders and interested parties to the Business Continuity Plan include:

- Staff.
- The local community.
- Business customers.
- Ofsted.
- Students and their families/carers.
- Health and Safety Executive.
- Charity Commission.
- Other suppliers, e.g., IT service providers, solicitors, auditors, etc.
- Department for Education.

General Details

Registered Name	Chesterfield College and its wholly owned subsidiaries: • Training Services 2000 Ltd (t/a Learning Unlimited Derby). • Recruit Unlimited Ltd. • Learning Unlimited ATA Ltd.
Registered Address	Infirmary Road, Chesterfield, S41 7NG, United Kingdom.
Company Registration Number	n/a
Business Description	College of Further Education and associated activities of subsidiary companies.
Subsidiary Companies	**Training Services 2000 Ltd** Based in Derby and trading under the name Learning Unlimited Derby. Located in two leasehold units at 11-13 and 15-21 Royal Scot Road, Pride Park, Derby, DE24 8AJ which comprise a mix of classrooms and workshops for engineering trades. The staff of TS2000 are employed by Recruit Unlimited Ltd and the centre is attended by 70-100 apprentices each day. This location is part of a range of modern industrial units.
	Recruit Unlimited Ltd Provides a general recruitment agency service to the college's own students and employs some college staff.
	Learning Unlimited ATA Ltd A company used for payroll purposes, predominantly for employing apprentices.
	Chesterfield College Enterprises Ltd Trading as The Lilypad Café – ceased trading.
	Chesterfield Technical Academy Ltd A dormant company.
Associated Companies	None.
Ethos / Vision / Aims	"To be recognised locally and nationally as an outstanding college by the students, employers, and communities we serve". We place our students at the centre of everything we do which is reflected in our key performance areas: • **People:** customer excellence, talented people, outstanding services. • **Position:** responsive, ambitious, educational business. • **Performance:** developing skills, achieving excellence, inspiring success. • **Prosperity:** financially sound, equipped to flourish. • **Progress:** driving ambition, enabling progression, maximising potential.
College History / Formation	The college was founded in 1841 as the Chesterfield and Brampton Mechanics' Institute, and went through various

	incarnations, including the merger in 1984 of Chesterfield Art College and Chesterfield College of Technology, before becoming Chesterfield College in 1993.
Ofsted Report / Rating	Rating is currently "Good" following a November 2022 inspection.
Activities	The college offers a wide range of traditional FE courses to 16-19-year-olds, basic skills training for students with learning difficulties, some 14-16-year-olds, and adult learners. It is also one of the leading providers of apprenticeships in the UK. Higher education courses are also provided. The upper floor of North Block 4 at Infirmary Road accommodates specialist teaching suites for autistic children, a service which the college has taken over from the council. Staff are fully qualified and there is an access lift at the west entrance. The college is one of the largest providers of apprenticeships in the UK. Catering is in-house. The college provides training in catering under its hospitality courses and there is a training restaurant which is open to members of the public. No outside catering is undertaken. College carries out 'deep cleans' of kitchen extraction systems. Queens Park Sports Centre, Boythorpe Road, Chesterfield, S40 2ND. This is a sports centre and ground in which the college has invested £2.5m to provide three classrooms and training rooms, together with sports facilities.
College Website	https://www.chesterfield.ac.uk/

College Details

Number of Governors	17
Number of Students	Approx. 11,000
Students Age Range	
Boarding Students	n/a
Catering	Catering is in-house. The college provides training in catering under its hospitality courses and there is a training restaurant which is open to members of the public. No outside catering is undertaken. College carries out 'deep cleans' of kitchen extraction systems.
Provision of First Aid and Healthcare Facilities	All security staff and caretakers are first aid trained, as are some technicians, and all sports staff have completed Sports First Aid. In total there are 15 first aiders, all of whom have completed the three-day course First Aid at Work. First aid is provided at all college events, including trips away as required.

	Circa 10 students require support administering medication. College claims funding for 75 high needs students, with varying levels of need.
Welfare Arrangements / Emotional Support etc.	The college has a Student and Apprentice Services Team which provides advice and guidance. A counselling service is available to students. Independent counselling and legal advice services are available to staff.
Is there any use of drones?	No.

General Site Information

Health and Safety Governance and Approach	The Principal has overall responsibility for Health and Safety within the college. The Safety, Health, and Environment (SHE) Manager is the 'competent person' appointed by the College Group under the Management of Health and Safety at Work Regulations 1999 and the position holds all relevant qualifications. There is a formal Health and Safety Committee that is represented at Corporation and Principalship level by the Assistant Principal Finance, IT and Estates. It meets on a termly basis or by arrangement.
Can you confirm that you have maintained an up-to-date accident and incident book?	Yes – accident report forms are completed by the individual or attending first aider.
Details of any lone working and risk management procedures implemented, if applicable.	Lone working is rare, but there is a lone working procedure in place and risk assessments are completed if required.
Facilities Management Resources	Yes
Last Insurer survey – focus and actions	
Do you have a written Health and Safety Policy?	Yes
Do any third-party companies assist with Health and Safety or risk management?	Hettle Andrews Risk Services: HA ONE and HA ONE+.
Is a specific employee responsible for Health and Safety and fully trained for this function?	Yes – see above.
Is documentary evidence of systems and procedures maintained?	Yes – management systems in place for Health and Safety, asbestos, and legionella.
Do risk assessments exist for each area of business activity?	Yes

Are Health and Safety audits completed. If yes, by whom and how often?	Internal audit schedule in place. External audits from Fire and Rescue Service, insurer, and HSE.
Do you have a document retention policy?	Yes
Have there been any prosecutions, prohibition notice, or improvement orders issued under Health and Safety legislation during the last 5 years?	No

Locations

Name	Address	Postcode	Use / Additional Property Details
Chesterfield College	Infirmary Road, Chesterfield	S41 7NG	Owned by the college.
Training Services 2000 Ltd	15-21 Royal Scot Road, Pride Park, Derby	DE24 8AJ	Leased premises by Training Services 2000.
Training Services 2000 Ltd	11-13 Royal Scot Road, Pride Park, Derby	DE24 8AJ	Leased premises by Training Services 2000.
Playing Fields	1 Langer Lane, Chesterfield	S40	Playing fields owned by the college, including football pitches and a changing room block.
1 Wharf Lane	1 Wharf Lane, Chesterfield	S41 7NE	Leased building, used as an MOT training centre.
2 Wharf Lane	2 Wharf Lane, Chesterfield	S41 7NE	Leased building, used for construction trades.
Queens Park Sports Centre	Boythorpe Road, Chesterfield	S40 2ND	Leisure centre run by Chesterfield Borough Council who sub-let, on a 25-year lease, rooms and access to Chesterfield College. The college has three classrooms based here and exclusive access to badminton courts and the gym during college hours. The Borough Council owns the buildings and all the equipment. The college are responsible for the classroom contents.

Construction

Building	Year	Walls	Floors	Stairs	Roof	Use
South Block Original	1927	Brick with some glass curtain walling	Concrete – 3 storeys	Concrete	Flat felt on concrete	Administration; classrooms; staff offices and rooms; stores; facilities on all floors. ICT on top floor, server rooms on top and ground floor. Online exam testing suites on top floor. 4x passenger/goods lifts in central core. Lift motor room on roof.
South Block Extension	1950s	Brick/block	Concrete – 9 storeys	Concrete	Flat felt on concrete	
South Block 'T' Extension	1960s	Brick/block	Concrete – 9 storeys with bridge over entry to car park	Concrete	Flat felt on concrete	
Central Block	1970s	Brick	Concrete – 3 storeys	Concrete	Flat felt on concrete; timber sub-layer	Main Reception; refectory; Taste on the Go; Café Central; Heart Space; Digital Centre; Careers; admin offices.
Sports Hall (part of Central Block)	1970s	Block with formed metal	Concrete – double height	Metal to mezzanine	Pitched formed metal	Sports facility.
North Block 1	1970s	Steel	Concrete – 3 storeys	Wood	Flat felt on concrete	Hair and Beauty; fashion; salons; fitness suite (open to public on first floor); general classroom and electrical training centre.
North Block 2	1970s	Brick, steel, and concrete frame	Concrete – 3 storeys	Concrete	Flat felt on concrete	Fashion; art and design; ICT (including Mac Suite on ground floor); photography (including dark rooms, studio, technical room, and store for equipment).

North Block 3	1970s	Brick on steel frame	Concrete – 3 storeys	Concrete	Flat felt on concrete	Art and Design; IT (Mac Suite on ground floor); design and technology; silver smithing and jewellery (braziers); dance studios with roof lights; lighting studio; recital room (also used for performances and has capacity for 144 seated) with control booth. Kilns located in this building.
North Block 4	1930s	Brick	Concrete – 3 storeys	Concrete	Pitched tile	Arches Café; IT learning centre; general classrooms; IT suites; Autism Centre; furniture store. ICT server room on first floor.
West Block (ex-grammar school; Grade II listed)	1870s	Brick	Concrete with some timber – 4 storeys	Mix concrete and timber	Pitched slate	Higher education; ESOL; IT rooms; general classrooms on upper floors; West Studios tenants.
East Block 1	2015	Brick	Concrete – 2 storeys	Concrete	PVC membrane, standing seam, composite panel	Carpentry; plumbing; painting and decorating workshop; carpentry machine shop; semi outdoor erection shop; IT and general classrooms.
East Block 2	1970s	Brick	Concrete – 2 storeys	Concrete	Flat felt on concrete	Engineering; laser cutting; welding booths (auto shut off on electric); plumbing; electrical workshops; IT and general classrooms.
East Block 3	1980s	Brick	Concrete – single storey	Concrete	Northlight	Auto engineering workshops; panel beating; spray booth; welding.
Wharf Lane 1	1970s	Brick	Concrete – single storey	None	Part flat felt/part pitched asbestos	MOT testing station; motor engineering in one large and one smaller workshop. Emergency electrical cut-off.

Wharf Lane 2	1970s	Brick	Concrete – 2 storeys	Concrete and timber	Part pitched tile/part pitched formed metal	Wet construction trades; roller shutter door for deliveries; mezzanine floor not used as deemed untested.
Langer Lane Sports Pavilion and field		Timber on brick/steel frame	Single storey	Concrete	Flat felt	Used as a changing facility for those playing sports on the sport fields.

Plan Copies

Chesterfield College recognises the importance of always having access to its Business Continuity Plan. The college has implemented a robust system for managing and maintaining its plan, which includes both printed and electronic copies.

Printed copies of the plan are held by members of the Senior Management Team and the continuity team. This ensures that key personnel always have access to the plan, including when internet access may be disrupted or unavailable. "Live" versions of the plan are held within an online system accessed via the college's insurance brokers, Hettle Andrews, and copies are also stored on the college intranet and cloud drives. This approach ensures that the plan is readily accessible to all key personnel, regardless of their location, and can be updated in real-time as necessary.

The online system is password-protected, and only authorised personnel have access to it. This provides an additional layer of security and ensures that the plan remains confidential and protected from unauthorised access.

Storing copies of the Business Continuity Plan in multiple locations is essential to ensure that the plan is readily accessible and can be accessed from different locations during emergencies. For example, if the college's main Infirmary Road site was inaccessible during a crisis, personnel could access the plan from other locations.

In addition to the online system, copies of the plan are also stored on the college intranet and cloud drives. This provides additional redundancy and ensures that the plan can be accessed from any device with internet connectivity. This approach also ensures that the plan is always up to date, as any updates made to the plan are automatically synchronised across all devices.

Regular testing and updating of the plan are also essential to ensure that it remains relevant and effective. The plan is regularly reviewed and updated to reflect changes in the operating environment and emerging threats to the college's operations. The college also conducts regular training sessions to ensure that personnel are familiar with the plan and their roles during an emergency. Effective communication and dissemination of the plan are also critical. All personnel, including employees, contractors, and suppliers, are informed of the plan and their roles and responsibilities during an emergency. This ensures that everyone is aware of the plan and can work together to implement it effectively.

By implementing these measures, the college is well-prepared to manage any disruptions and maintain its operations while mitigating risks to staff, clients, and other stakeholders.

Review and Update of the Plan

Plan owners and persons responsible for the maintenance and review of this document are the Principal and CEO, Assistant Principal Finance, IT and Estates, and various heads of department with support from senior management and members of the continuity team, as required. All such individuals also have a responsibility to raise awareness of the Business Continuity Plan and provisions in place for handling major incidents and recovery/continuity of services. This plan will be formally reviewed on at least an annual basis as an 'intellectual' review exercise to identify changes or amendments that may be required. Scenario-based testing of the plan will

also be undertaken every 12 months to two years, in addition to functional tests of the key technical resources such as IT systems and backups and restoration of data.

Drills or test exercises will also be undertaken from time to time; however, this will be less frequent in view of the significant disruption and cost associated with these exercises. Following any test exercise, review, or real activation of the plan, an incident log will be maintained, and a formal debrief will be held with the continuity team to establish any shortcomings or lessons to be learnt so improvements and amendments can be made to the plan to ensure the continuous improvement of the plans in place.

It is essential that the Business Continuity Plan remains accurate, effective, and up to date. As such, it is important to both test the plans and to review them on a regular basis. By monitoring the risks faced on an ongoing basis the college will be able to react quickly to changing threats or exposures to make the necessary changes to the plans. It is also important to monitor changes within the college, such as changes in activities or processes carried out, equipment and premises used, and changes of supplier, which can impact upon the contingency plans laid down in this policy. As such, the college has put in place monitoring processes including:

- **Internal audit and review:** a formal 'intellectual' review of the policy and plans to identify amendments that may be required. This will be undertaken on an annual basis by the continuity team.
- **Test, exercise, or rehearsal:** these test scenarios will involve staging a live test to establish whether the provisions included in the plan come together. Time and cost to complete these are higher, but they test the logic behind the plan and confirm that the people involved, and the timescales set down, would work in the event of a real incident. This will be handled as a 'desk-based' process whereby all the necessary checks are completed via telephone, internet, and email.

If the college does have a real situation to respond to, an incident log will be maintained, and it will be treated as a learning experience. The college maintains a log of all incidents (whether test or real) and communications during the incident, so it can be reviewed afterwards to look for lessons that can be taken forward.

The outcome of any test or review undertaken will lead to corrective action being taken and changes implemented, whether they be policy related, administrative, physical, financial, technology or communications related. Each minor amendment or course of corrective action taken will contribute to the continual improvement of the college's business continuity management provisions and makes the college more robust for future events.

Continuity Team

Following a major incident, the continuity team will be called together to make an initial assessment of the nature of the event and the likely impact and duration of the disruption caused, which will assist in deciding whether the Business Continuity Plan needs to be formally invoked. If this is necessary, the members of the team have their own distinct areas of responsibility, as identified below:

Area of Responsibility	Name	Role / Title
Executive Lead	Julie Richards	Principal and CEO
Executive Deputy	Claire Godfrey	Deputy Principal

Operational Oversight	Thomas Kidsley	Assistant Principal Finance, IT and Estates
Quality and Curriculum	Michaela Greaves	Assistant Principal Teaching, Learning and Quality Improvement
Safeguarding	Jo Down	Assistant Principal Student Experience and Wellbeing
Facilities and Estates	Eric Hadley	Director of Facilities and Estates
IT Services	Matthew Prime	ICT Technical Manager
Business Intelligence Systems		
Exams	Cheryl Atkins	Head of Quality Assurance
Enrolments	Joe Fojut	Head of Information Services
Data Protection	Jo Gibson	Data Protection Officer
Health and Safety	Roger Mitchell	Safety, Health and Environment Manager
Communications	James Marples	Head of Brand and Communications

In the event of a major incident occurring or being declared, the continuity team will meet to assess the nature of the event, the impact, and likely duration. The team will determine if this constitutes a 'major incident' and whether the Business Continuity Plan should be initiated. A valid quorum of the continuity team comprises at least four members of staff; one of whom will be a representative from the Senior Management Team. Other members will ideally represent Facilities and Estates, IT Services, and Communications as identified above. One of these individuals will act as the team leader and in practice this may rotate between these senior staff members, as required. Continuity team members must be available for invocation in the event of a major incident on a 24/7 basis. If not personally available, each must ensure that other members of their team can provide appropriate cover for them.

Area of Responsibility	**Role Description**
Executive Lead / Executive Deputy	• Inform the continuity team of the scale and scope of the emergency and/or disaster. • Organise a base from which to work. • Schedule team meetings as appropriate. • Ensure all aspects of the emergency and recovery are handled effectively and properly. • Inform the DfE, OfS etc. as appropriate.
Operational Oversight	• Immediately inform the insurance broker/company of the emergency and/or disaster. • Liaise and communicate with the Loss Adjustor appointed by the insurers. • Inform the appropriate bodies of the type and scale of the emergency and/or disaster. • Identify and request assistance from these bodies as and when required.

Quality and Curriculum	• Ascertain the loss of or damage to course materials and loss of examination data. • Ascertain whether the emergency and/or disaster has reduced accommodation required to sit examinations. • Identify other curriculum issues affected by the emergency and/or disaster. • Identify curriculum requirements both immediate and long term to enable complete reinstatement of curriculum delivery.
Facilities and Estates	• Ascertain the amount of damage to premises and equipment (other than IT equipment). • Plan and oversee the salvage of college assets/property and identify premises and equipment requirements both immediate and long term to enable complete college operations to be reinstated. • Place orders for and oversee the supply of equipment, temporary buildings/accommodation, and long-term building projects. • Ensure, in conjunction with the Police, the site and buildings are secure, utilising the required resources (human and equipment).
IT Services	• Ascertain the extent of damage to computer hardware, software, wiring, servers, and communications etc. • Identify requirements for essential computer functions to be operative as soon as possible and what is required to reinstate all functions as were operative prior to the emergency and/or disaster occurring. • Place orders for and oversee the supply and installation of the equipment etc. identified above, having liaised with those responsible for insurance claim and recovery financing.
Communications	• Compile and issue all communications to the media – such communications having been agreed by the Principal and CEO. • Answer all enquiries from the media or direct such enquiries to the Principal and CEO, if required. • Inform staff that all media enquiries should be directed to the person responsible for media liaison and under no circumstances will they be answered by other members of staff. • Identify such information that should not be released – such communications having been agreed by the Principal and CEO.

Threat and Risk Analysis

Analysis and assessment of the risks facing the college, which could threaten the continuity of college operations, is of utmost importance and is continually reviewed to ensure that any changing risks are tackled immediately. All continuity team members are also required to remain vigilant to these threats and risks. Therefore, whilst the following risks have been considered in the development of this Business Continuity Plan and will be formally reviewed on an annual basis, the development of this plan is not the beginning and end of the process. Analysis of continuity threats and risks is an ongoing and recurring process.

The risk assessment process that has been followed involves the discussion and consideration of each of the risk scenarios identified, with input from senior management of the college and members of the continuity team. The risk rating calculated for each threat is a combination of the 'likelihood' of it occurring, multiplied by the potential consequences of that incident, or its potential 'severity'.

Both 'Likelihood' and 'Severity' are ranked as High, Medium, or Low, each of which corresponds to a numerical value of three, two or one, respectively. These are then multiplied to come up with the risk rating which is also expressed as being High (representing scores of six or nine), Medium (being scores of three or four) or Low (being scores of one or two). This methodology is described by the risk rating matrix included below:

Likelihood	High (3)	**3**	**6**	**9**
	Medium (2)	**2**	**4**	**6**
	Low (1)	**1**	**2**	**3**
		Low (1)	Medium (2)	High (3)
		Severity / Consequence		

Each of the threats/risks considered as part of the business impact analysis have been outlined in the table below, which also highlights the risk ratings calculated for each, as well as the decision as to whether the college intends to put in place disaster and continuity plans for each of the threats. This has been created with careful review by the continuity team.

Threat or Risk	Likelihood	Severity	Risk Rating
Loss of premises	Low	High	3
Loss of key staff	Low	Medium	2
Loss of equipment/machinery	Low	High	3
Loss of utilities	Low	High	3
Loss of IT/telecommunications	Low	Medium	2
Loss of transport	Low	Medium	2
Loss of suppliers	Low	Medium	2
Regulatory action	Low	High	3
Fraud/theft	Low	Medium	2
Hacking/data loss/computer virus	Medium	High	6
Hazardous spillage/pollution	Low	Low	1
Infectious disease	Medium	Medium	4
Loss of catering	Low	Medium	2

Of the 13 risks reviewed, one was identified as being high risk and five areas were seen as being a 'Medium' risk. For each of these, the college intends to put in place formal recovery plans. For one of the items graded as a 'Low' risk (loss of IT/telecommunications) it is still desirable to

have a formal plan for this crucial area and plans already exist for cyber risks. The following two areas of risk are, for the purposes of developing a recovery plan, being treated as one item:

- Hacking/data loss/computer virus.
- Loss of IT/telecommunications.

The final area of risk which has been flagged as needing a formal recovery plan is regulatory action (and the associated reputational damage that could result). In terms of the areas that are not going to form part of the Business Continuity Plan, some further commentary and justification is included below. This reflects areas where the risk rating has been calculated as 'Low', where the event is unlikely, or it would not have a significant impact on the continuity of the organisation.

Loss of Key Staff

This was deemed to be a low risk, as deputies exist for all positions and there is a relatively large staff with a good level of competence in all areas. Succession plans are in place, staff training is provided and, where possible, upskilling of deputies is pursued. From the point of view of a larger group of staff being out for a period (in the event of a widespread illness), this is not seen as a significant concern.

Loss of Transport Services/Infrastructure

It is noted that this would only be relevant significant to road closures. Most students are transported by public transport. For any road closures the drivers would follow diversions in place set up by the council. This is a low-risk concern.

Loss of Key Suppliers

Under this heading the suppliers that would have the most immediate impact would include curriculum resources, however there are multiple suppliers available. The only other significant category of supplier would be in respect of construction projects for new buildings or for refurbishments. However, these would tend to be part of a tender process, including significant due diligence checks and contractual guarantees and would be overseen by the college's landlords.

Financial Fraud or Theft

This is an area that is heavily scrutinised, with limits set for individuals in terms of what they are allowed to sign off. It is agreed that there is no means by which a significant amount could be taken that would cause lasting damage to the organisation.

Environmental Hazards, Spillages or Pollution

This has limited relevance to the college. Whilst there are some hazardous substances stored and used, these are generally in small quantities and have very little chance of entering water courses or ground water. Purchasing controls also exist and COSHH assessments are completed for new substances.

Loss of Catering

The college has two fully equipped kitchens and a catering firm that supplies all meals.

Organisational Analysis

Following analysis of the different threats/risks and consideration of the risk rating and supplementary discussions, the decision has been made to develop formal recovery plans for the following scenarios:

- Loss of premises.
- Loss of equipment/machinery.
- Loss of utilities.
- Regulatory action (and associated reputational damage).
- Loss of IT services or hacking/data loss/virus.
- Infectious diseases.

These are discussed further below and take account of the areas/departments on which they could have an impact. Each of the functions/departments have also been assigned a priority level, defined as either 'critical', 'urgent', or 'non-urgent', and a Maximum Tolerable Period of Disruption (MTPD) timescale to set out how long the college could reasonably continue to operate with that function being disrupted.

Loss of Premises

The recovery process itself is set out in the Loss of Premises disaster plan. The functions that would be affected by this threat/risk are listed below, along with their respective priority and MTPD:

Risk Rating: Medium		
Functions Affected	**Function Priority**	**MTPD**
Academic departments	Urgent	24 hours
IT functions	Urgent	24 hours
Administration/office	Urgent	24 hours
Kitchen	Non-Urgent	30 days
Site support	Non-Urgent	15 days

Loss of Equipment/Machinery

The recovery process itself is set out in the Loss of Equipment/Machinery disaster plan. The functions that would be affected by this threat/risk are listed below, along with their respective priority and MTPD:

Risk Rating: Medium		
Functions Affected	**Function Priority**	**MTPD**
Academic departments	Urgent	24 hours
IT functions	Urgent	24 hours
Administration/office	Urgent	24 hours
Kitchen	Non-Urgent	30 days
Site support	Non-Urgent	15 days

Loss of Utilities

The recovery process itself is set out in the Loss of Utilities disaster plan. The functions that would be affected by this threat/risk are listed below, along with their respective priority and MTPD:

Risk Rating: Medium		
Functions Affected	**Function Priority**	**MTPD**
Academic departments	Urgent	24 hours
IT functions	Urgent	24 hours
Administration/office	Urgent	24 hours
Kitchen	Non-Urgent	30 days
Site support	Non-Urgent	15 days

Regulatory Actions

The recovery/management process itself is set out in the Regulatory Action disaster plan. The functions that would be affected by this threat/risk are listed below, along with their respective priority and MTPD:

Risk Rating: Medium		
Functions Affected	**Function Priority**	**MTPD**
Academic departments	Urgent	24 hours
IT functions	Urgent	24 hours
Administration/office	Urgent	24 hours
Kitchen	Non-Urgent	30 days

Loss of IT or Hacking/Data Loss/Virus

The recovery process itself is set out in the Cyber disaster plan. The functions that would be affected by this threat/risk are listed below, along with their respective priority and MTPD:

Risk Rating: High		
Functions Affected	**Function Priority**	**MTPD**
Academic departments	Urgent	24 hours
IT functions	Urgent	24 hours
Administration/office	Urgent	24 hours

Infectious Diseases

The recovery process itself is set out in the separate Infectious Diseases Disaster Recovery Plan. The functions that would be affected by this threat/risk are listed below, along with their respective priority and MTPD:

Risk Rating: Medium		
Functions Affected	**Function Priority**	**MTPD**
Academic departments	Urgent	24 hours
IT functions	Urgent	24 hours
Administration/office	Urgent	24 hours
Kitchen	Non-Urgent	30 days
Site support	Non-Urgent	15 days

Insurance Coverage

In the event of an incident occurring which requires the implementation of the Business Continuity Plan, one of the most important factors in ensuring that swift and effective action will be taken is ensuring that adequate financial resources are in place to put the recovery plan into effect. For the most part, the college will be reliant on the insurance arrangements in place to provide for this.

Risk	Current Insurer
Education Combined	Travelers Insurance Company Ltd
Combined Liability	AXA Insurance UK plc
Commercial Engineering	Allianz Insurance plc
Computers	Allianz Insurance plc
Cyber Liability	NMU (Speciality) Ltd
Hired-In Plant	Allianz Insurance plc
Motor Fleet	QBE Insurance Group
Personal Accident and Travel	Allianz Insurance plc

The cover matrix can be found below:

Policy Response	Loss of Premises	Loss of Equipment or Machinery	Loss of Utilities	Regulatory Action	Loss of IT or Hacking / Data Loss / Virus	Loss of Catering Facilities
Education Combined	Reinstatement of premises and revenue loss	Reinstatement of premises and revenue loss	Loss of revenue and expenses	N/A	N/A	Reinstatement of premises and revenue loss
Management Liability	N/A	N/A	N/A	Legal expenses cover and legal advice	N/A	N/A
Computers	N/A	Repair and replacement of computers affected	N/A	N/A	N/A	N/A
Cyber Liability	N/A	N/A	N/A	N/A	Restoration of systems and security	N/A

Material Damage

Buildings:

Building Name	Risk	Cover Basis	Sum Insured (Declared Value) (£)
All declared owned buildings	Buildings	Reinstatement (day one 25%)	97,767,899 (78,214,319)
15-21 Royal Scot Road	Tenants improvements	Reinstatement (day one 25%)	66,406 (53,125)

11-13 Royal Scot Road	Tenants improvements	Reinstatement (day one 25%)	22,004 (17,603)

Contents:

Location	Content Name	Cover Basis	Sum Insured (Declared Value) (£)
All declared college buildings	Machinery, plant, and all other contents	Reinstatement (day one 25%)	28,197,500 (22,558,000)
All declared college buildings	3D printers, laser cutter, and associated equipment	Reinstatement (day one 25%)	558,863 (447,090)
All declared college buildings	Wines, spirits, and tobacco	Indemnity	1,000
All declared college buildings	Deterioration of stock – any one loss or occurrence	Indemnity	10,000
All declared college buildings	Deterioration of stock – single unit limit	Indemnity	1,000
All declared college buildings	Motor vehicles whilst in the workshop	Indemnity	250,000
All declared college buildings	Stock	Indemnity	51,000
UK wide	Property in transit	Indemnity	100,000
EU	Property in transit	Indemnity	25,000
EU	Goods at exhibitions and shows	Indemnity	25,000
Territorial limits	Promotional trailer	Indemnity	10,000

Business Interruption

Item Description	Location	Limit (£)	Indemnity Period (Months)
Gross revenue first loss limit	All declared locations	3,000,000	36
Additional increased costs of working	All declared locations	3,000,000	36

Management Liability

Item Description	Limit of Liability (£)	Excess (£)
Governors and officers/trustees liability	2,000,000	n/a
Legal liability	5,000,000	10,000
Employment practices liability	100,000	10,000

Crime	1,000,000 in the aggregate per policy year	10,000
Legal pursuit	100,000	1,000
Regulatory advice service	Included	-

Cyber Liability

Item Description	Limit of Liability (£)	Excess (£ or hours)
Cyber response	250,000	2,500
Cyber restoration	250,000	2,500
Cyber expense	250,000	2,500
Court attendance costs • Directors and Officers rate per day • Employees rate per day	 500 250	 - -
Cyber extortion	250,000	2,500
Business interruption	250,000	8 hours
Cyber crime	250,000	2,500

Insurance Claims Process

The college's insurance broker will be contacted in the first instance, in order that they can instruct a suitable loss adjuster to visit the site as a matter of urgency in the event of a significant loss, as well as reporting the matter to the college's insurance company. The college's designated contact details are listed below:

Client Manager

Jock Brindley
T: 0121 423 6203
M: 07968 906006
E: Jock.brindley@hettleandrews.co.uk

Client Advisor

Chris Stanford
T: 0121 423 6211
M: 07968 906 007
E: chris.standford@hettleandrews.co.uk

Claims Advisor

Charles Eurell
T: 0121 423 6226
M: 07960 932 203
E: charles.eurell@hettleandrews.co.uk

Risk Management Executive

Ian Morgan
T: 0121 423 6217
M: 07951 267 690
E: ian.morgan@hettleandrews.co.uk

Capital Reserves Cash

Outside of insurance arrangements, the college also holds healthy financial/capital reserves, which could potentially be called upon to supplement the insurances in the event of interruption to continuity due to infectious diseases and the loss of key staff, which are no longer insurable events.

ISO 22301 Alignment

This accreditation supports businesses of all sizes build a Business Continuity Management System (BCMS) and instantly communicates that the business has a reliable and stable continuity plan.

ISO 22301 allows business continuity managers to self-audit their organisation's business continuity plan and make sure it meets the standards set out by ISO 22301. The college does not have to become formally certified; ensuring that the business continuity plan holds up against the regulations set out in ISO 22301 is enough to demonstrate to stakeholders that the college is well prepared for a disaster scenario.

Appendix A: Loss of Premises Disaster Recovery Plan

Examples of short-term loss of premises could include an emergency fire evacuation, bomb threat, or gas leak which would all require evacuation and a temporary 'Denial of Access' from the building. Longer term 'Denial of Access' events might include widespread flooding that prevents access to the building, or the premises being under investigation as the scene of a crime which could make it inaccessible for hours or days whilst forensic evidence is collected.

Long term loss of premises would most likely be caused by serious damage to the fabric of the buildings, such as fire, explosion, or flooding, which would take weeks or months before the site could be cleared prior to commencement of repair and/or rebuild.

Phase 1: Identification, Discovery and Warning

The college has several measures in place to provide adequate warning of incidents and/or a reliable means of identifying or detecting a problem:

- A robust Fire Risk Assessment has been completed and is reviewed annually to minimise the risk of a fire occurring.
- A fire detection and alarm system are installed at all buildings, which will enable early identification and evacuation in the event of a fire.
- The fire detection and alarm system are linked to a monitoring station, which will ensure that the fire service is notified immediately, therefore minimising damage to the building in the event of a fire.
- There is some security in place at the entrance, which minimises the risk of unwanted visitors to the site who could cause damage to the buildings etc.
- There are locks fitted on all exterior doors with a key card entry system or key lock system.
- Loss of communications also acts as a warning and discovery method.
- The Designated Safeguarding Lead and Deputies act as a safeguarding provision for staff and students.

Phase 2: Emergency Evacuation

Please refer to the Emergency Evacuation Plan and Procedures document. It is noted that some events may require students to be contained in an area for safety concerns, as noted with the procedures.

Phase 3: Assess the Damage and Notify Insurers

Emergency Contact	Role	Phone Number	Email Address
Charles Eurell	Claims Director	07960923203	Charles.eurell@hettleandrews.co.uk

Once the initial emergency is under control, everyone is safe, and the premises has been secured as best it can be, the business continuity team will survey the damage (where relevant). This will be a two-fold exercise:

1. To establish the extent of the disruption and which areas or facilities are, and will remain, out of action. Also, to establish which facilities are still operational and can remain in

use. All key decisions to be relayed and arranged by the Principal (or senior manager deputising) who has operation oversight.

2. The level of physical damage to the premises will need to be assessed from an insurance point of view, so a report of the incident and likely level of damage can be made to the insurance company to start the process of repair.

Phase 4: Implementation of Emergency Home Learning

In the event of the premises being unavailable the business continuity team will review all courses with some being switched to virtual home learning for students assessed to cope with this change. Lesson plans and schedules will be transposed into Microsoft Teams and similar programmes. Noting that staff may not be familiar with these programmes, external training may be sought and funded by the insurance programme. Such training is estimated to take approximately 3 days. Laptops and dongles will be sourced for staff with limited access to the internet.

With the support of the insurance programme, the college will ensure that each student is provided with a correctly scoped laptop, including a dongle device where appropriate. It is noted that any use of home learning cannot be a long-term solution. Any course where home learning is not feasible will require temporary classrooms. Bearing in mind some student's needs, home visit lessons will be facilitated for those students where remote home lessons are not feasible or applicable.

Phase 5: Interim Arrangements

Once the event and any subsequent damage have been assessed by the business continuity team, a decision will be made to adopt interim arrangements in the short, medium, or long term:

Loss of Premises	Actions Required
Short term (<1 week)	Business continuity team move to alternate rooms. All other staff to work from home as directed by the business continuity team.
Medium term (<6 weeks)	Lessons moved to a remote learning experience with the support of the IT infrastructure. Funding used will be provided by the insurance programme.
Long term (>6 weeks)	The business continuity team will work with brokers to arrange rebuild/refurbishment of the existing premises and/or purchasing and fitting of new premises.

In the event temporary classrooms are needed, the college has identified Bunkabin (www.bunkabin.co.uk; 0345 456 7899) as its supplier. They provide portable units to those in higher education, including providing additional student accommodation and classrooms to institutions. They can serve universities, schools, and learning centres and will be able to meet the college's needs.

Phase 6: Building Restoration

Almost immediately after the college's property has been damaged by fire the insurance repair technicians and adjusters will take over, alleviating the college of the responsibility of fixing the premises post-fire. As such it is important to immediately contact the broker Hettle Andrews, Claims Director, Charles Eurell on 07960 923203. Once they arrive, they will begin the repair process, which includes using techniques approved by the restoration industry.

- **Initial Inspection:** after the fire has been extinguished, a qualified inspector will account for the extent of the damage and determine what repairs need to be done, including structural damage repairs. Depending on the type of damage done, the college may need to hire multiple different professionals funded by the insurance programme, such as roofers, carpenters, carpet installers, and plumbers. In this case, hiring a general contractor to oversee the fire repair process may be necessary.
- **Safety and Prevention:** after the initial inspection and assessment of fire damage to the property, the fire restoration experts will isolate and block off unsafe areas to prevent injury or further damage. Blocking off these areas also protects the college from liability, such as if anyone were to injure themselves from the various dangers present.
- **Soot and Debris Removal:** after a fire it is likely the premises will be affected by soot and will be overwhelmed by smoke smell. Fire repair technicians quickly work to remove soot and smoke, as well as other debris. During this initial clean-up process, they will scrub the walls and ceilings of soot and apply deodorisation products to handle odour removal using air-scrubbing technology. They will also sort through contents and leave salvageable belongings aside for restoration.
- **Water Removal and Sanitisation:** once the initial debris, smoke and soot have been removed and it is safe for technicians to proceed, water damage restoration technicians will remove standing water and dry out the affected area. Specialised equipment, such as air movers, fans, and dehumidifiers prevent mould growth, help to disinfect the site, and minimises further damage to the property's structure. The fire restoration team may use various cleaning agents to salvage furniture, upholstery, flooring, drywall, and other items impacted by smoke, soot, and water. They will also neutralise any lingering odours and dispose of items that are beyond saving.
- **Repair Damage:** repairing the damage done to property is the final step in restoration. This step involves reconstructing any physical structure damage.

Phase 7: Insurance Funding

Material Damage

Building Name	Risk	Cover Basis	Sum Insured (Declared Value) (£)
All declared owned buildings	Buildings	Reinstatement (day one 25%)	97,767,899 (78,214,319)
15-21 Royal Scot Road	Tenants improvements	Reinstatement (day one 25%)	66,406 (53,125)
11-13 Royal Scot Road	Tenants improvements	Reinstatement (day one 25%)	22,004 (17,603)

Business Interruption

Item Description	Location	Limit (£)	Indemnity Period (Months)
Gross revenue first loss limit	All declared locations	3,000,000	36

Additional increased costs of working	All declared locations	3,000,000	36

Appendix B: Loss of Equipment Disaster Recovery Plan

The scale of effect for loss of equipment, machinery, or contents can vary greatly depending upon the importance of the item in question and the length of time missing. Examples of short-term losses might include the malfunction of an office laptop where replacements are readily available, or a lost electrical tool that can be replaced easily at a local department store. Larger and longer-term losses tend to involve more significant or bespoke equipment where there is a reliance on its continued operation, or specialist setup (such as servers) is required. Specialist equipment can be both expensive and have extensive lead times if they are shipped across the globe.

Given the above variance of possible effects, the college's contingency and continuity plan caters for multiple eventualities and scenarios. All options must be considered to minimise disruption and to enable the college to continue to operate. The below phases have been highlighted for implementation in the event of a disaster:

Phase 1: Notification of Claim

Emergency Contact	Role	Phone Number	Email Address
Charles Eurell	Claims Director	07960923203	Charles.eurell@hettleandrews.co.uk

Once the initial emergency is under control, everyone is safe, and the premises has been secured as best it can be, the business continuity team will survey the damage (where relevant). This will be a two-fold exercise:

1. To establish the extent of the disruption and which areas or facilities are, and will remain, out of action. Also, to establish equipment which is still operational and can remain in use. All key decisions to be relayed and arranged by the Principal who has operational oversight.
2. The level of physical damage to the equipment will need to be assessed from an insurance point of view, so a report of the incident and likely level of damage can be made to the insurance company to start the process of repair.

Phase 2: Identify Critical Equipment

Identifying the critical items for immediate replacement is the start point and most important part of the continuity planning process for this risk. The business continuity team have identified equipment that is heavily relied upon and needs to be immediately sourced because there is a heavy business reliance, where losses would be incurred rapidly if it was out of use for any period. This includes computer resources and immersive interactive equipment. This is a non-exhaustive list.

Phase 3: Temporary Replacement of Critical Equipment

Often critical equipment will have a lead time and as such the next step is arranging to obtain temporary replacements to ensure continued operations. In this regard the college has considered:

- Arrangements for immediate short-term lease of replacement machinery/equipment. The business continuity team should refer to the college's supplier list.

- The availability of second-hand machinery as a cost-effective solution, rather than waiting for new. The college should explore the second-hand market in conjunction with the insurance programme.
- Where space constraints and finances allow, holding redundant, replacement equipment in store for contingency arrangements.

Phase 4: Repair Processes

Once key equipment has been identified, the college will work with the insurance providers to facilitate repair and remedial actions. If the works can be conducted 'in-house' the college will acquire material via its supplier network. If the works need to be outsourced, contractors will be engaged.

With external arrangements for machinery maintenance, breakdown, and repair, it will be possible to put in place contractual agreements on response times and repair times. Where repair is not feasible or would not be recommended due to the equipment being old, obsolete, or of low value, the only option may be for replacement, which is expanded on below in Phase 5 of the plan.

Phase 5: Replacement

In the event of equipment being damaged beyond repair and needing to be completely replaced, access to equipment specifications is essential and the format in which they are stored needs to be secure. Equipment specifications should be physically secure, stored in multiple locations, in an electronic format, or a geographically remote location to ensure that they are always available in an emergency. The business continuity team should revert to the college's online and physical storage.

Phase 6: Insurance Funding

Material Damage

Location	Content Name	Cover Basis	Sum Insured (Declared Value) (£)
All declared college buildings	Machinery, plant, and all other contents	Reinstatement (day one 25%)	28,197,500 (22,558,000)
All declared college buildings	3D printers, laser cutter, and associated equipment	Reinstatement (day one 25%)	558,863 (447,090)
All declared college buildings	Wines, spirits, and tobacco	Indemnity	1,000
All declared college buildings	Deterioration of stock – any one loss or occurrence	Indemnity	10,000
All declared college buildings	Deterioration of stock – single unit limit	Indemnity	1,000

All declared college buildings	Motor vehicles whilst in the workshop	Indemnity	250,000
All declared college buildings	Stock	Indemnity	51,000
UK wide	Property in transit	Indemnity	100,000
EU	Property in transit	Indemnity	25,000
EU	Goods at exhibitions and shows	Indemnity	25,000
Territorial limits	Promotional trailer	Indemnity	10,000

Business Interruption

Item Description	Location	Limit (£)	Indemnity Period (Months)
Gross revenue first loss limit	All declared locations	3,000,000	36
Additional increased costs of working	All declared locations	3,000,000	36

Appendix C: Loss of Utilities Disaster Recovery Plan

Like all organisations, the college is critically reliant on utilities such as electric, gas, and water. It is imperative that recovery plans are put in place to mitigate the effects of any losses, and to ensure continuity of services are resumed as quickly as possible. One way to improve the resilience of the organisation by ensuring there should never be a full loss of power is to ensure that the power source that different operations rely upon is not the same. The recovery options are outlined in further detail below.

Electricity supply: initially all functions will suffer because of an electricity outage, whether that be a complete cease of operations or operating at a reduced capacity. Whilst direct teaching may be facilitated in some areas it would be manifestly unsafe to continue teaching in the absence of heating, alarm systems, and security. The college is reliant on an electrical supply for light, heat, telephones, computers, etc. Without power it could be completely out of service for the duration of the power loss. In addition to this downtime, there can be secondary issues such as data losses, loss of students, and an eventual impact on revenue. In the event of an extended power outage the following should be prioritised:

1. IT infrastructure.
2. Curriculum activity.
3. Student services.
4. Finance.

Disruption will be minimised if the continued operation of these integral parts of the college can be quickly established.

Oil supply: oil supply is generally relied upon to provide heating in a premises. In most locations it is less of a concern than a loss of electricity, however it will still disrupt operations. At an extreme level, operations would have to cease completely, and if there was a loss of oil-fired heating it could render the premises uninhabitable during periods of low temperatures. The priority is to identify processes that are dependent on an oil supply, such as heating, hot water, and cooking or catering provisions. The college would source a temporary power supply for the duration of the outage. Once critical functions have been identified they will be prioritised to allow more effective planning of the continuity response. Due to the nature of heating, this will be seasonally dependent.

Water supply: from a health and safety legislation perspective, if the college is unable to provide sanitary conveniences and a source of portable water, it cannot operate as a place of business or education.

Phase 1: Identify the Source of the Failure

A loss of utilities at the college could be caused on the college site or because of supply failure from the mains. The first issue when a loss is experienced is to establish where the fault or damage is, so it can be established whether it is something for the college to tackle internally, or whether the problem has been caused by suppliers or the network.

If it is an internal problem, the college will arrange for repairs as soon as possible either via in-house engineers or via contractors, possibly in cooperation with insurers if it is connected to an insurance claim.

Contact details for the electricity and gas suppliers and the local water board can be found online so they can be contacted in an emergency to establish what the fault is, if it is on the mains network, and to get an estimate on the time for which supplies will be disrupted.

Phase 2: Notification of Claim

Emergency Contact	Role	Phone Number	Email Address
Charles Eurell	Claims Director	07960923203	Charles.eurell@hettleandrews.co.uk

Once the initial emergency is under control, everyone is safe, and the premises has been secured as best it can be, the business continuity team will survey the damage (where relevant). This will be a two-fold exercise:

1. To establish the extent of the disruption and which areas or facilities are, and will remain, out of action. Also, to establish equipment which is still operational and can remain in use. All key decisions to be relayed and arranged by the Principal who has operational oversight.
2. The level of physical damage to the equipment that will need to be assessed from an insurance point of view, so a report of the incident and likely level of damage can be made to the insurance company to start the process of repair.

Phase 3: Consider Recovery Options

Source	Actions required
Electrical Supply Failure	For repairs of electrical faults in-house, an electrician will need to be employed. If there is not one on the staff currently, a contractor will need to be used. Utilising an external contractor will also negate the need to hold spare parts. Details of the contractor is held on file. • Contact the supplier to confirm outage time. • Contract an electrician to identify source and power requirements. • Hire portable generators and have the electrician connect the supply to key areas. • Arrange for a refuelling system. • Arrange for any repairs to the electrical equipment damaged. See Appendix B.
Oil Supply Failure	The primary options for a back-up oil supply will vary on the required usage and the connections that are available. Again, these are available via storing the requisite supplies on-site so they always remain available or putting in place a contract of supply to ensure that someone else can deliver on these needs in the event of an oil supply failure. Depending on the level and nature of the use, portable pressurised oil cylinders may be adequate (whether they are held on site or supplied as required), or alternatively bulk storage tanks on-site or mobile storage will need to be arranged. Contact details for the relevant suppliers are outlined within this document.

	Again, if there is no qualified oil engineer employed on-site, it may be necessary to arrange for one to be available to switchover supply lines, etc.
Water Supply Failure	The provision of water supplies in an outage can range from bottled water from the local supermarket to tankers holding thousands of gallons. The precise details of the scenario will determine whether adequate supplies can be stored on site, or whether outside arrangements will be needed. Emergency water supplies can be obtained from multiple suppliers and may be arranged by the water board if the fault is under their control. Whether this is adequate for the college's purposes or not will need to be assessed. As well as the provision of water for drinking and washing, other sanitary facilities will need to be considered when calculating the college's requirements. It may also be necessary for the college to arrange for the supply of portable toilets, where the emergency water supply cannot be used to supply the existing facilities.

Phase 4: Insurance Funding

Business Interruption

Item Description	Location	Limit (£)	Indemnity Period (Months)
Gross revenue first loss limit	All declared locations	3,000,000	36
Additional increased costs of working	All declared locations	3,000,000	36

Appendix D: Regulatory Action Disaster Recovery Plan

This is an area that is regularly underestimated as a continuity risk, and yet is the one area that could shut down the college immediately and potentially permanently. Most of the college's regulatory bodies can place restrictions on the college, including financial and other sanctions that would be prohibitive to trading. It is therefore of vital importance that the college guard against these continuity risks. The extent and type of regulator to which the college has exposure will vary depending on the department, but the process will be similar for each, with the focus on preventing action to begin with:

- Seeking immediate advice from Hettle Andrews to ensure funding for legal defence costs.
- Establishing who the relevant regulators are for the problem.
- Determining what action can be taken against the college for failure to comply, and the continuity risks this poses.
- Establishing what the college's responsibilities are under the regulator's remit and/or how to achieve compliance by taking considered legal advice.
- Working with the insurance programme to put in place plans and compliance functions to ensure that the college operate within the legal and regulatory guidelines during the process of discovering, investigating, and reacting to a breach.

Phase 1: Identify Potential Regulators

Whilst not an exhaustive list, regulatory bodies to which the college may be exposed include the following:

- Health and Safety Executive and/or Local Authority.
- Office for Students.
- Fundraising Standards Board.
- Ofqual.
- Food Standards Agency and/or Environmental Health Office.
- Equility and Human Rights Commission.
- Care Quality Commission.
- Department for Education.
- Police and Crown Prosecution Service.
- Information Commissioner's Office.
- Financial Conduct Authority.
- Environment Agency.
- Security Industry Authority.
- Public Health England.
- Ofcom.
- Charity Commission.
- Ofsted.

Phase 2: Notification of Claim

Emergency Contact	Role	Phone Number	Email Address
Charles Eurell	Claims Director	07960923203	Charles.eurell@hettleandrews.co.uk

Once the initial emergency is under control, everyone is safe, and the premises has been secured as best it can be, the business continuity team will survey the damage (where relevant). This will be a two-fold exercise:

1. To establish the extent of the disruption and which areas or facilities are, and will remain, out of action. Also, to establish equipment which is still operational and can remain in use. All key decisions to be relayed and arranged by the Principal who has operational oversight.
2. The level of physical damage to the equipment that will need to be assessed from an insurance point of view, so a report of the incident and likely level of damage can be made to the insurance company to start the process of repair.

Phase 3: Isolate Disruption from Regulatory Action

The powers of different regulators vary widely. However, there are some common themes to consider in mitigating the ramifications of potential actions:

- Action notices, which empower the regulator to make the college take certain action to do something.
- Prohibition notices to make the college stop doing something that is contrary to regulations.
- Improvement notices to change the way the college is doing something, to come into line with regulations or best practice.
- Carry out investigations into college activities (and place prohibitive restrictions on trade during this time).
- Close certain elements of the organisation, or the whole organisation, permanently.
- Prosecute the college for carrying out criminal actions.
- Cancellation or restriction of funding, or access to existing financial resources.
- Financial penalties against the college and/or, in a personal capacity, Directors or Senior Managers of the college.
- Expulsion of key personnel from the college, imprisonment of key personnel, or creation of a temporary loss of personnel who are required to take part in a court case, hearing, or trial.

Phase 4: Response

In response to such disruption, the college have secured access to solicitors via its Legal Expenses Cover. They can represent the college in all types of investigation and prosecution, including those brought by the Police, HM Revenue & Customs, the Health and Safety Executive, Local Authorities, the Environment Agency, the Care Quality Commission, Ofsted, and the Information Commissioner's Office. They also have a wealth of experience in the criminal courts, the coroners court, and before tribunals and inquiries. The nature of the work is such that the college may need urgent advice in a crisis.

Phase 5: Insurance Funding

Item Description	Limit of Liability (£)	Excess (£)
Governors and officers/trustees liability	2,000,000	n/a
Legal liability	5,000,000	10,000
Employment practices liability	100,000	10,000
Crime	1,000,000 in the aggregate per policy year	10,000
Legal pursuit	100,000	1,000
Regulatory advice service	Included	-

Appendix E: Cyber Disaster Plan

As part of the insurance programme, the college have full access to the services of ReSecure. They are an integrated data breach response service, available through the college's cyber insurance, created to provide a 'one-stop shop' for the full range of services required to manage, investigate, and recover from a cybersecurity incident.

The ReSecure operating model provides local capability with international reach and collaboration, giving clients a flexible solution, both in terms of scale and specialism, equipped to suit the college's requirements.

Over many years ReSecure have helped hundreds of organisations of all sizes to investigate and recover from a range of damaging and criminal cyber incidents. They stand ready to assist college teams to minimise the impact on business operations and reputation if the college falls victim to a cyber incident. They will be appointed and funded by the insurance programme to assist with the below action plans:

Emergency Contact	Role	Phone Number	Email Address
Charles Eurell	Claims Director	07960923203	Charles.eurell@hettleandrews.co.uk

Insurance funding:

Item Description	Limit of Liability (£)	Excess (£ or hours)
Cyber response	250,000	2,500
Cyber restoration	250,000	2,500
Cyber expense	250,000	2,500
Court attendance costs • Directors and Officers rate per day • Employees rate per day	 500 250	 - -
Cyber extortion	250,000	2,500
Business interruption	250,000	8 hours
Cyber crime	250,000	2,500

Recovery Action Plan: Ransomware

Phase 1: Notification of the Insurance Claim

- Once Ransomware has bypassed antivirus and other defences it is likely the result of some user action (like clicking a link), but this is not always the case. The virus is using the infected user's permissions to access and encrypt files. Ransomware can encrypt operating system files, network shares and even cloud file systems.
- There is a small chance the college will be able to decrypt these files with a free tool, available online from several different security companies. This best-case scenario will still result in hours of downtime and is effective only on specific ransomware variants. In most cases the college will be forced to restore files from backup. Recovery of large data sets can take from several hours to several days to complete. As such the college should immediately notify the insurance brokers to seek assistance from the insurance programme. Now is a good time to communicate to executives and staff that there is

a problem. Critical systems will be down for an extended period. This can be done using the external SMS service.

Phase 2: Lockdown of Systems

- Currently, all that is known is that college systems are infected. One or more users may be the source. The infection may be hours or days old. The college will need to take the shares offline immediately. Before these shares are locked, it might be possible to save a lot of time in later steps. The college will look at the open files on the encrypted shares. This can help identify the source of the infection, called Patient Zero. If one user has hundreds of open files, they are probably the source of the infection.
- Which shares should be locked? All of them is the safest answer, but the situation will dictate which ones should be restricted. There are too many factors to include in this guide. Locking the shares will stop the progress of the encryption, if it is still underway, and will prevent other shares from being encrypted until the infection is removed from the network.

Phase 3: Shutdown Patient Zero

- It is critical to identify and shut down the source of the infection. As a larger organisation this can be very difficult. Once identified, the college will review who is the owner of the new files (instructions for decryption)? What permissions were needed to modify the encrypted files? Who has those permissions?
- Once the college has identified patient zero and acted quickly it is possible to limit the infection. In some cases, the infection will not be noticed until whole shares are encrypted. The college will turn all potentially infected machines off and disconnect them from the network for the duration. Until the machines are fully cleaned, they continue to pose a threat to network security and could cause re-infection.

Phase 4: Identify the Infection

- The next step is to identify the variant so the college can plan the best recovery option for the situation. Critical note: most of the ransomware variants have a timer that starts when the link is clicked in the instructions file. In some cases, the ransom doubles when time is up. In other cases, the files have been encrypted forever. Do not click the links without referral to ReSecure.
- These files are the key to working through the infection. By searching the web for the text in these files, it is usually possible to determine the variant. Each variant has critical characteristics that must be researched. For some variants there are decryption tools. Other variants may not even have encrypted the files but are still demanding the ransom.

Phase 5: Decrypting

- It is recommended that the college use a one-time use virtual machine that is severely locked down and hardened for decryption. Once the decryption is complete, the virtual machine will be destroyed. This will dramatically slow down the process of decryption, as opposed to running the tool directly on the file servers. Though antivirus/malware solutions are not effective at preventing the infection, many are effective at identifying

the decryption tool as malware. This can complicate the decryption process and may require extra time to work through.

Recovery Action Plan: Malware

Phase 1: Notification of the Insurance Claim

- Once malware has bypassed antivirus and other defences it is likely the result of some user action (like clicking a link), but this is not always the case. The virus is using the infected user's permissions to access and encrypt files. Malware can encrypt or corrupt operating system files, network shares and even cloud file systems.
- There is a small chance the college will be able to decrypt these files with a free tool, available online from several different security companies. This best-case scenario will still result in hours of downtime and is effective only on specific malware variants. In most cases the college will be forced to restore files from backup. Recovery of large data sets can take from several hours to several days to complete. As such the college should immediately notify the insurance brokers to seek assistance from the insurance programme. Now is a good time to communicate to executives and staff that there is a problem. Critical systems will be down for an extended period. This can be done using the external SMS service.

Phase 2: Lockdown of Systems

- One or more users may be the source. The infection may be hours or days old. The college will need to take the shares offline immediately.
- Before these shares are locked, it might be possible to save a lot of time in later steps. The college will look at the open files on the encrypted shares. This can help identify the source of the infection, called Patient Zero. If one user has hundreds of open files, they are probably the source of the infection. Locking the shares will stop the progress of the encryption, if it is still underway, and will prevent other shares from being encrypted until the infection is removed from the network.

Phase 3: Shutdown Patient Zero

- It is critical to identify and shut down the source of the infection. As a larger organisation this can be very difficult. Once identified, the college will review who is the owner of the new files (instructions for decryption)? What permissions were needed to modify the encrypted files? Who has those permissions?
- Once the college has identified patient zero and acted quickly it is possible to limit the infection. In some cases, the infection will not be noticed until whole shares are encrypted. The college will turn all potentially infected machines off and disconnect them from the network for the duration. Until the machines are fully cleaned, they continue to pose a threat to network security and could cause re-infection.

Phase 4: Identify the Infection

- The next step is to identify the variant so the college can plan the best recovery option for the situation.

- These files are the key to working through the infection. By searching the web for the text in these files, it is usually possible to determine the variant. Each variant has critical characteristics that must be researched. For some variants there are decryption tools.

Phase 5: Decrypting

- It is recommended that the college use a one-time use virtual machine that is severely locked down and hardened for decryption. Once the decryption is complete, the virtual machine will be destroyed. This will dramatically slow down the process of decryption, as opposed to running the tool directly on the file servers.
- Though antivirus/malware solutions are not effective at preventing the infection, many are effective at identifying the decryption tool as malware. This can complicate the decryption process and may require extra time to work through.

Recovery Action Plan: DDoS Attack

Phase 1: Notification of the Insurance Claim

- In terms of the college servers, the college needs to be able to identify when it is under attack. This is because the sooner the college can establish that problems with the website and services are due to a DDoS attack, the sooner the college can stop the DDoS attack.
- To be able to do this, the college is familiar with its typical inbound traffic profile; the more the college knows about what its normal traffic looks like, the easier it is to spot when its profile changes. Most DDoS attacks start as sharp spikes in traffic, and it is helpful to be able to tell the difference between a sudden surge of legitimate visitors and the start of a DDoS attack. As soon as an attack is identified the college will notify the insurance programme.

Phase 2: Overprovision Bandwidth

- It generally makes sense to have more bandwidth available to the web server than the college is ever likely to need. That way, sudden and unexpected surges in traffic resulting from an advertising campaign, special offer, or mention in the media can be accommodated. Even if the college created overprovision by 100% or 500%, that likely will not stop a DDoS attack, but it might give the college a few extra minutes to act before resources are overwhelmed completely.

Phase 3: Defend at the Network Perimeter

- There are a few technical measures that can be taken to partially mitigate the effect of an attack, especially in the first minutes, and some of these are quite simple.
- The college will rate limit its router to prevent the web server from being overwhelmed.
- The college will add filters to tell the router to drop packets from obvious sources of attack.
- The college will timeout half-open connections more aggressively.
- The college will drop spoofed or malformed packages.
- The college will set lower SYN, ICMP, and UDP flood drop thresholds.

- While these steps have been effective in the past, DDoS attacks are now usually too large for these measures to be able to stop a DDoS attack completely. The most the college can hope for is that they will buy a little time as a DDoS attack ramps up.

Phase 4: Call the ISP or Hosting Provider

- The college stands a better chance of withstanding a DDoS attack if the web server is located in a hosting centre. This is because its data centre will likely have far higher bandwidth links and higher capacity routers than the college has, and its staff will probably have more experience dealing with attacks. Having the web server located with a host will also keep DDoS traffic aimed at the college's web server off the corporate LAN.
- If a DDoS attack is large enough, the first thing a hosting company or ISP is likely to do is "null route" traffic, which results in packets destined for the college's web server being dropped before they arrive.

Phase 5: ReSecure Experts

- For very large attacks, it is likely that the best chance of staying online is to use a specialist DDoS mitigation company. These companies have large-scale infrastructure and use a variety of technologies, including data scrubbing, to help keep websites online. ReSecure will contact a DDoS mitigation company directly, or the college's hosting company or service provider may have a partnership agreement with one to handle large attacks.

Recovery Action Plan: Social Engineering

Phase 1: Notification of the Insurance Claim

- Social engineering attacks exploit misplaced trust, not stupidity. If someone fools the college's staff, it is because they are good at manipulation, not because staff are stupid. All staff are potential victims, and as social engineering campaigns get increasingly sophisticated, the risk is only going to increase. In the event of an attack, Hettle Andrews will recover lost amounts under the policy, but the college will have to ensure no reoccurrence. It is essential that staff are aware of their security responsibilities and report potential phishing attacks rather than think that saying something will get them into trouble. This will save the college valuable time when responding to an incident.

Phase 2: Learn the Psychological Triggers

- Recognising social engineering attacks is not always as easy as identifying obviously dubious emails. Social engineering takes many guises and attackers exploit a number of psychological triggers to get past people's natural defences.
- As well as developing trust and gathering intelligence that they can later use, they might create situations of false urgency and heightened emotion, such as fear, excitement, and panic, to confuse their victim, exploit their victim's propensity for reciprocation by creating a sense of indebtedness, or rely on people's conditioned responses to authority. Learning to recognise such tactics is essential.

Phase 3: Retrain Staff

- It is important post-event to train staff so that they understand the consequences of social engineering attacks and are suspicious of unsolicited communications and unknown people.
- Check whether emails genuinely come from their stated recipient (double-check sender's names and look out for giveaways such as spelling errors and other illiteracies).
- Do not open suspicious email attachments.
- Beware of tailgating and do not be rushed (attackers will create a sense of urgency to pressure their victim).
- Think before providing sensitive information. Check a website's security before submitting information, even if they seem legitimate (avoid websites that use HTTP).
- Pay attention to URLs and 'typo squatting' (sites that look genuine but whose web address is subtly different from the legitimate site it is imitating).

Phase 4: Test the Effectiveness of the Training

- As well as retraining staff, it is important to test the effectiveness of training measures. Simulated phishing attacks will give the college a good idea of staff susceptibility to phishing emails.

Phase 5: Implement Appropriate Technical Measures

- Adequate resources, funds, materials, and staff training is essential, but it is not everything. The college also needs to implement wider information security measures so that if attackers do manage to trick users, it is difficult for them to get much further.
- The college will use firewalls, antivirus, antimalware, whitelisting, and spam filters to keep malicious traffic to a minimum, applying patches and keeping systems up to date so that the college is not vulnerable to known software and network vulnerabilities.
- The college will use rigid data classification models and privileged access management policies to secure and control who has access to sensitive data, keeping records of who has access to what information, and who is therefore most at risk.
- The college will implement a policy of using strong unique passwords. The information security standard ISO 27001, which sets out the requirements of a best-practice information security management system, provides essential guidance relating to the suggestions above. Annex A to ISO 27001 provides 114 security controls that any organisation can use to address the information security risks it faces, whether or not it opts to pursue certification to the standard.

Critical Function Tasks

Safeguarding	• **Phase 1:** contact vulnerable learners and external agencies to advise how to make contact (e.g., cannot contact via email) • **Phase 2:** message to staff about reporting safeguarding concerns. Use external systems if still available and provide mobile phone numbers. Contact social services to provide liasion points for queries/communication during the distruption.

	• **Phase 3:** collect securely stored paper contact details and work remotley using college laptops. • **Phase 4:** arrange for message on website regarding safeguarding queries, as college phones may be unavailable. • **Phase 5:** regular checks of vulnerable learners to continue. Use of paperbased forms to record student interactions.
Exams	• **Phase 1:** Exams Manager will provide a clear message of what has occurred, what systems are unavailable, and set priorities for the next week, and possibly month, with consideration to the following factors: exam registration, exam claims, visitors, audits, internal/external deadlines. • **Phase 2:** inform staff (including part-time invigilators) with a clear message, including a stock message of what to say if contacted by internal/external people. Awarding Bodies will be notified, and will require web portal access password reset (access may be restricted for a period of time). • **Phase 3:** online exams postponed. Exams Team will rebook exam when it is possible, assuming information in EBS is not lost, in which case new exams booking would be required. • **Phase 4:** paper based exams may go ahead if the building is open, with the exception of any access arrangements which require PCs. A member of the Exams Team would need to be on site 8am-3pm to receive post (exam papers and certificates) from Awarding Body. • **Phase 5:** results/certificates delayed until system is working.
HR and Payroll	• **Phase 1:** establish the current position of the payroll cycle. If payroll is due to process in the next 48 hour period a decision would need to be made in terms of what should be processed. • **Phase 2:** communication issued to staff to advise them of this and advise overpayments/underpayments would be rectified. This communication would need to take place via phone if email is unavailable. Line managers would filter queries for key issues. • **Phase 3:** communicate with third party organisations to ensure they are aware of the circumstances and to discuss payments. Stamps would need to be purchased if there was urgent mail to be sent. • **Phase 4:** the college would process payments as per the previous month going through MHR or the college bank. • **Phase 5:** paper copies of that month's changes would be available to determine potential significant under/overpayments for salaried staff. A business objects report could be run for the payments which were due to be processed to establish the difference for hourly paid staff.
Finance	• **Phase 1:** inform team members of attack using contact information sheet in the safe.

	• **Phase 2:** issue laptops from finance pool if remote working required. • **Phase 3:** retrieve memory stick from IT if access to reports not available (this will be a checked memory stick to ensure free from virus).

Appendix F: Infectious Disease Disaster Recovery Plan

It is now established precedent that outbreaks of infectious disease could shut down the college immediately and potentially for the foreseeable future. The college holds a separate escalation document which is accessible by all our teams. Most local and national regulatory bodies could place restrictions on the college, including restriction to premises and social distancing measures that could be prohibitive to activities. It is therefore of vital importance that the college guard against these continuity risks. This plan outlines high level measures while expecting the potential for future bespoke measures:

- Adequate resources, funds, and materials. The college will seek immediate advice from Radar Law on 0800 955 6222 and Hettle Andrews to ensure correct legal and health and safety advice is applied.
- Determine what action can be taken against the college for failure to comply and the continuity risks this poses.

Phase 1: Identify Regulator's Instructions

This is by no means an exhaustive list, but common regulatory bodies that may enforce restrictions to college premises in the event of outbreaks of infectious disease. Upon receipt of instructions from the following bodies the college must update its risk assessment and implement closure:

- Health and Safety Executive
- Local Authority
- Department for Education
- Government mandate/legislation
- Food Standards Agency
- Environmental Health Office
- NHS Trusts
- Police

Phase 2: Communicate Closure

Upon establishing a legal requirement to restrict access to college premises the college will immediately communicate this development to all stakeholders. This includes parents, students, staff, suppliers, and all other stakeholders. This should be by any reasonable means, including but not limited to phone calls, emails, social media, and website announcements.

Phase 3: Implementation of Emergency Home Learning

In the event of the premises being unavailable the college will review its courses, with some being switched to virtual home learning for students assessed as able to cope with this change. Lesson plans and schedules will be transposed into Microsoft Teams and similar programmes. Noting that staff may not be familiar with these programmes, external training may be sought and funded by the insurance programme. Such training is estimated to take approximately 3 days. Laptops and dongles will be sourced for staff with limited access to the internet. With the support of the college's insurance programme, the college shall ensure that each student is provided with a correctly scoped laptop, including a dongle device where appropriate.

The college notes that any use of home learning cannot be a long-term solution. Any course where home learning is not feasible will require temporary classrooms. Bearing in mind some student's needs, home visit lessons will be facilitated for those students where remote home lessons are not feasible or applicable.

Phase 4: Return to Site with Potential Control Measures

- Health and safety is a key consideration in all strategic planning. Social distancing minimises contact and mixing between people and reduces transmission. The college will aim is to reduce the number of contacts between students and staff within the setting. This will be achieved, as far as is reasonably practicable, through keeping groups separate (in 'bubbles') and through maintaining a social distance between individuals of one metre plus. A balanced approach between both these measures will be taken and kept under review to ensure students and staff are protected. The aim is to ensure students and staff can maintain a safe distance without the need to wear PPE (unless this is required). However, it is recognised that for certain groups of students and staff social distancing will not be achievable owing to their needs. In such cases the above groups of students and staff (including support staff providing 1 to 1 support) are considered as being within a distinct learning group or 'bubble'. As such their contact with other groups will, as far as is reasonably practical, be limited and therefore the risk of transmission minimised.
- The college will aim to form distinct learning groups (bubbles) that, as far as is possible, are separate from each other during the day and do not mix, to limit the transmission of the virus by limiting the number of students and staff in contact with each other to only those within the group. It also makes it quicker and easier in the event of a positive case to identify those who may need to self-isolate.
- Where possible, students will be grouped together into smaller consistent groups or cohorts (such as distinct year or level groups) with teaching staff dedicated to a specific group to reduce the number of contacts between students and staff. Support staff providing 1 to 1 support for a student would also be within that distinct learning bubble. Each distinct group or bubble will be instructed to stay apart as far as is possible from other groups and movement around site will be minimised to limit mixing. This will, as far as is possible, be accommodated in timetables. The college will minimise the movement of staff between cohorts where this is practically possible.
- There may be a need to reduce some class sizes on-site to ensure that social distancing can be maintained in learning spaces. Determining the size of classes will be dependent on various factors, including the number of students on a course and the physical dimensions of each teaching space. The college will review and determine where these may need to be reduced to ensure a safe and secure learning environment for students and staff. The college envisage that the delivery of the curriculum will need to include some blended learning, which will be provided via a combination of face-to-face teaching and remote learning. Where required, the college will provide appropriate webcams and/or other technology in learning spaces as needed.
- Contact between individuals will be reduced by ensuring, as far as is reasonably practicable, that students and staff only mix in distinct learning bubbles throughout the working day. The aim is to ensure that daily staff and student numbers at each college site are managed accordingly to ensure social distancing whilst also providing a full curriculum of learning. This will be facilitated, as far as possible, by timetabling each groups' attendance at college at timed and staggered periods throughout the day to

limit numbers of staff and students on campus at any one time. This will also consider the possibility of students waiting outside classrooms in corridors before lessons begin.

Appendix G: Communication Guidelines

Good communications are critical to the success of the college, especially in the event of a disaster when normal operations may be suspended, and the existing communications systems may not be viable. The college still needs to communicate with people in these situations, both inside and outside of the organisation, but it is vital that the right messages are communicated, at the right time, to the right people. In view of this, the college has strict guidelines on communications during an incident, which have been sub-divided into staff communications, parent, student, and supplier communications, and media communications.

Staff Communications

Who? Who does the college need to communicate with; is it all staff simultaneously or just selected people or groups e.g., managers or supervisors? The Crisis Management Team will be the first staff members to be contacted, and it may be necessary to designate a spokesperson to arrange staff communications, or to split up the responsibility via use of a communication tree with pre-determined lines of communication. The Crisis Management Team will know how best to respond to any queries that arise and will also have a better understanding of what the college want to achieve and what the forward plan is, so they will be the best people to agree on the content of communications and crucially who to convey the message to.

How? In the short term this will depend on what methods of communication are still available following the incident. This could be limited to mobile phones or emails. Once the options have been considered, the most practical and effective means should be used to communicate the agreed message to staff. If more than one method is easily available to use, then they should all be used, as people may not pick up on all communications sent to them. A dedicated means of communication, for example via the Incident Management Area of the college's business continuity management software, could be used. Or perhaps an enquiry line with a recorded message or an emergency number so staff can call the college to get the updated position.

When? As soon as possible. Staff are a key group of people that the college need to interact with early in the incident, as they will be the ones turning up to site not knowing what the current situation is. The college will need to continue staff communications as things develop to keep them up to date. It is also important to de-brief staff after an event to request confirmation of whether there were problems or whether things could have been done better.

What? Initially it will be a case of notifying staff of the incident and what they need to do in the short term e.g., stay at home until further notice, report to an alternative location, or login to the incident notice board online for further updates. Following this it will be necessary to keep staff informed of timescales and changes to locations etc., with a view towards getting back up and running at full capacity.

Parent, Student, and Supplier Communications

Who and How? All staff should be briefed on what the message is for parents, students, and suppliers, and what they should and should not say. If any member of staff has a particularly close relationship with individual parents, students, or suppliers, they should be the one to break the news as opposed to a stranger. These are key relationships that need to be nurtured, so getting the right person to speak to them is of paramount importance. The college need to control the communication. If the college fails to proactively advise parents, students, and

suppliers, they will either be alienated and go elsewhere or may end up putting extra pressure on staff who will have to field the calls and enquiries coming in from them.

When? Ideally parents, students, and suppliers will know prior to any public press release. This will not always be possible if it stirs the interests of the local or national press, but as far as possible parents, students, and suppliers should be prioritised. Furthermore, the college should prioritise important parents, students, and suppliers and speak to them directly. This will give a higher chance of them listening and the college being able to provide reassurance to them. Regular updates will also be important as things develop to keep them in the loop.

What? The communication will be honest but remain upbeat and positive. A key objective is to provide reassurance that the college is on top of things and has plans in place to get back up and running as soon as possible with minimal disruption to normal business activities. If the college has a degree of certainty over them, it can also advise of timescales. The college should avoid giving uncertain or exaggerated messages.

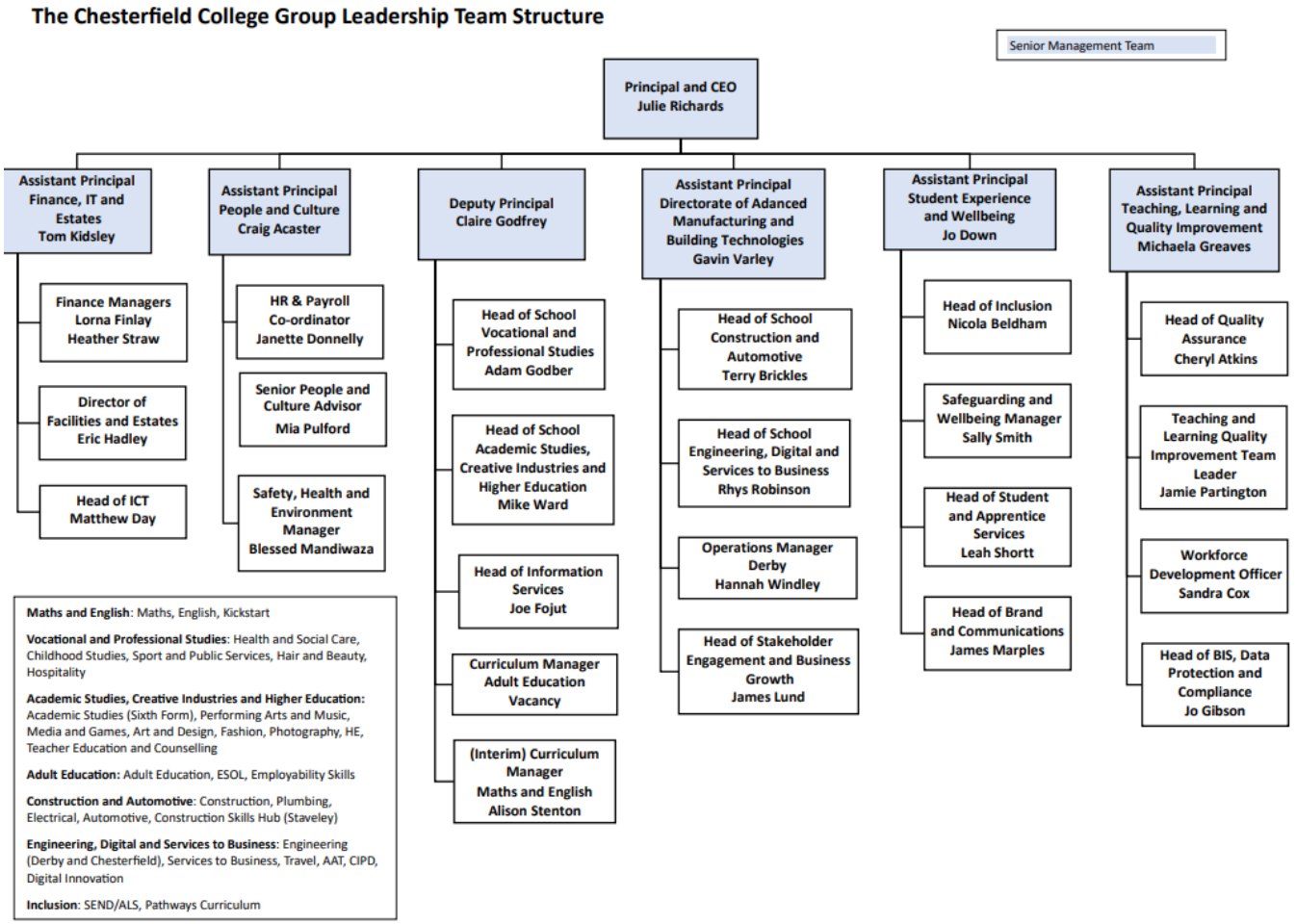
Media Communications

Who? This job should be reserved for trained spokespersons that, preferably, have experience of dealing with the media. This is likely to be a senior member of staff, who will then become the nominated contact towards whom all media enquiries should be directed. More importantly **all** staff members should be immediately advised that they are not allowed to speak to anyone about the incident, especially the media, face to face, via phone or text, or on social media.

When? After staff, governors, parents, students, and suppliers have been advised. Once all these key people have been advised a statement may be released to the media. This does not mean to say media cannot be contacted in the interim, however this should be contained to advising them of a time and through which medium the college will be providing a statement. It may also be a good idea to establish what areas the media are interested in or what questions they have so the college's spokesperson can be fully prepared.

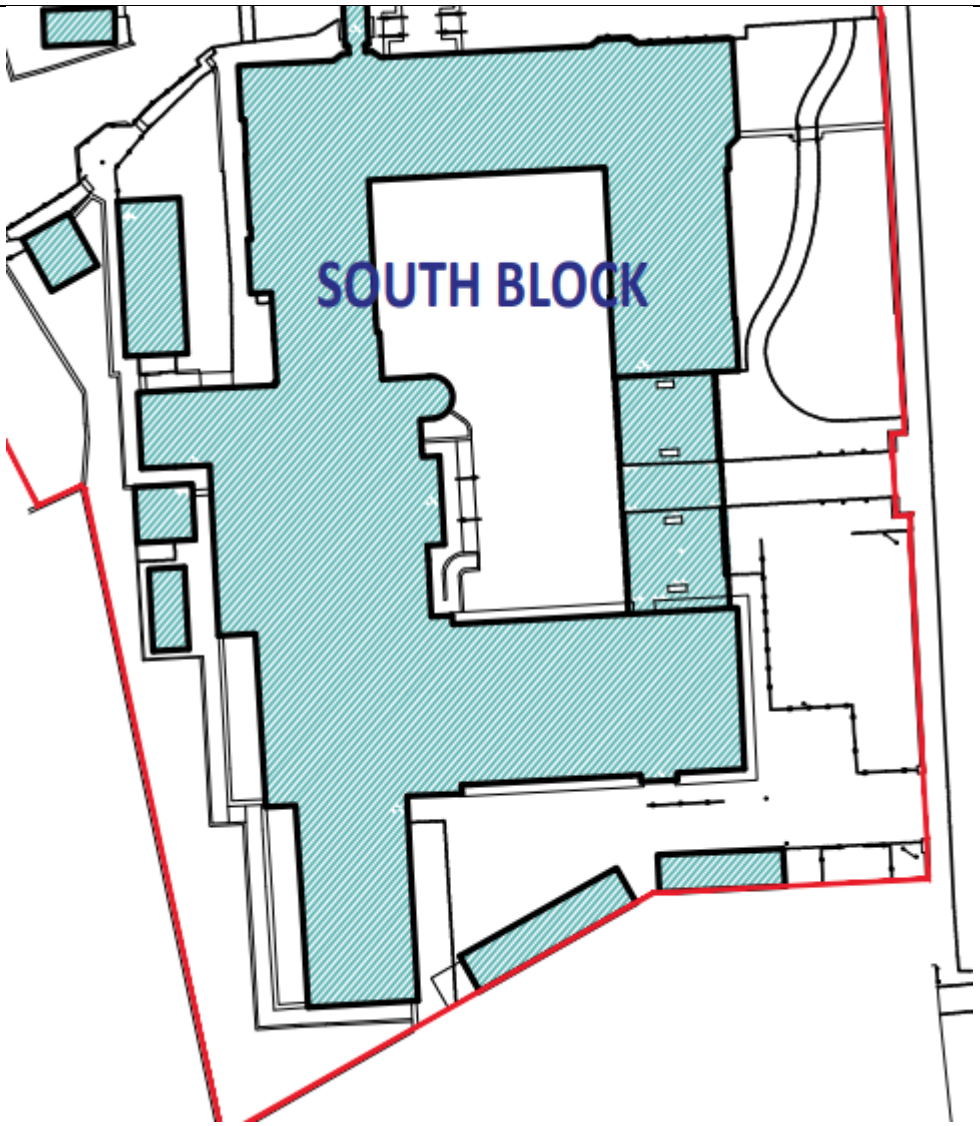
What? A press release should be agreed upon with input from senior management, and this should act as a script for the spokesperson in any interview. This will need updating as things develop. Crucially, no opinions on, or admission of liability for, the incident should be made. If the college have access to any media or PR consultants, guidance should be sought from them to ensure that the college is on the right track with its proposed release. Any interviews or statements issued should be restricted to the content of the agreed press release or script, with little or no deviation being made from this. The college should not give any opinions or make any assumptions and should refuse to answer ambiguous or leading questions that could cause the spokesperson to waver from the message they are trying to convey. The communication should remain informative, factual, and to the point, demonstrating that the college is in possession of the facts and remains in control of the situation.

Appendix H: Corporate Structure



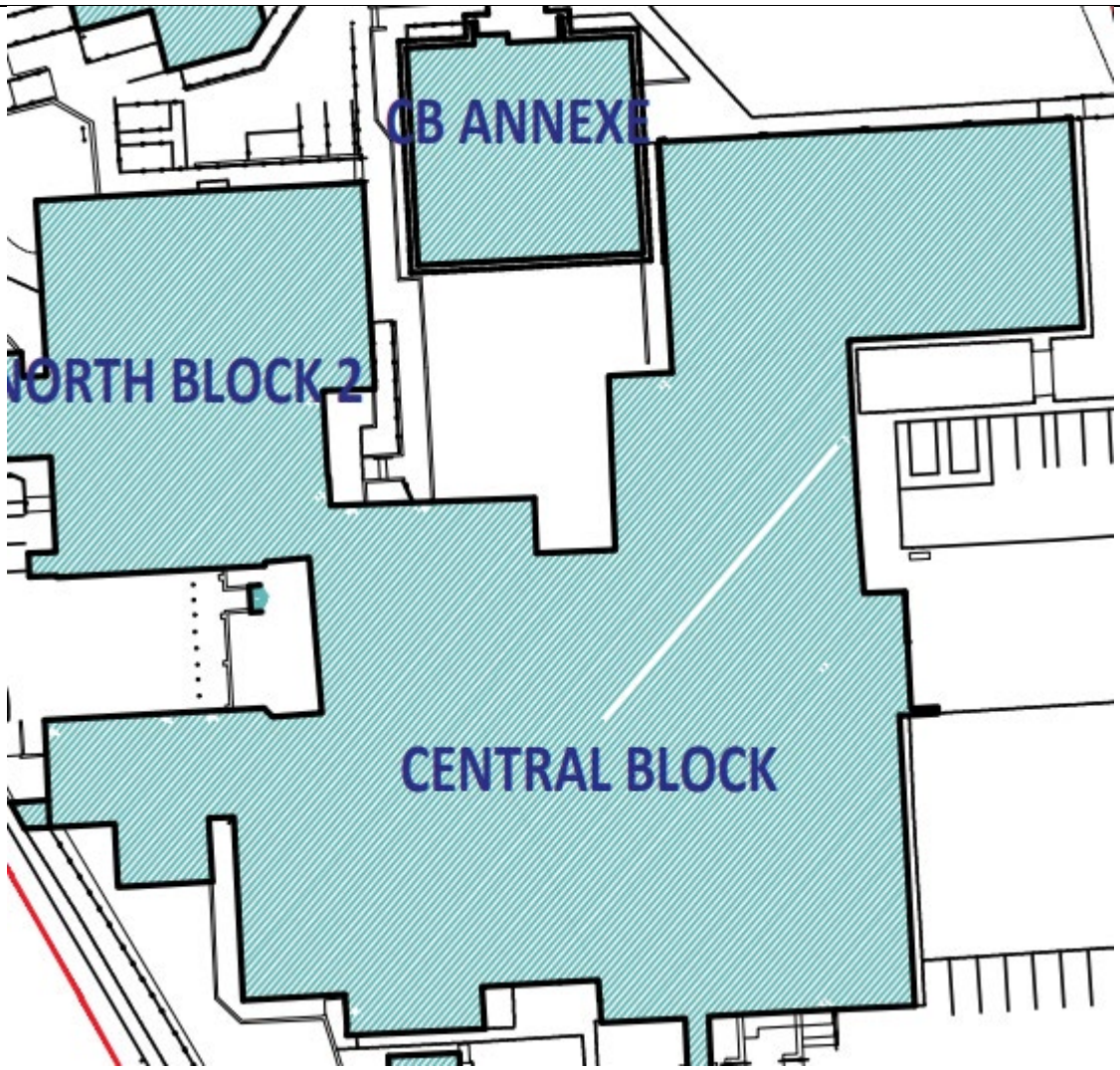
Appendix I: Building Continuity Register

South Block



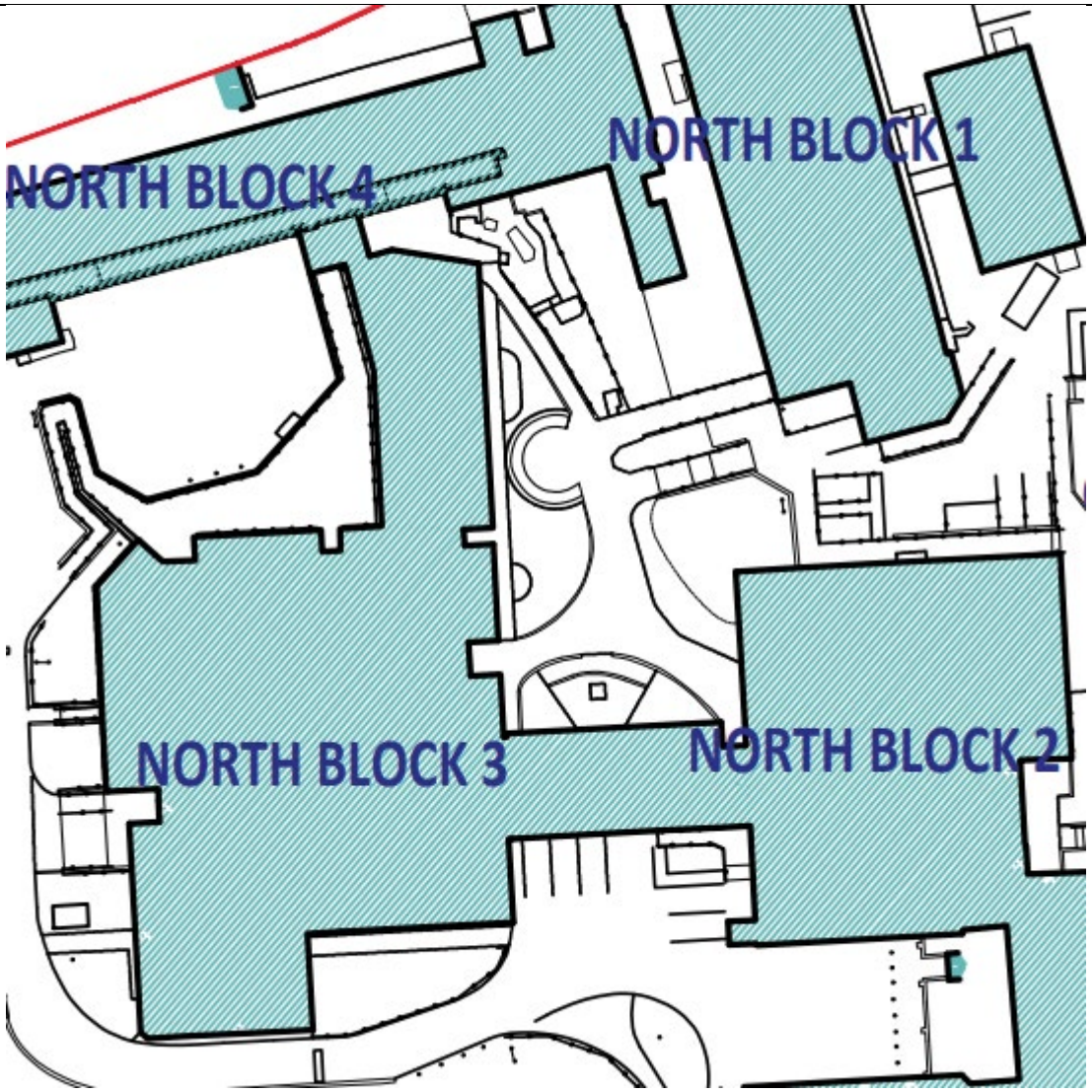
Space Requirement	Month							
	1-3 Months	3 – 6 Months	7 – 9 Months	10 – 12 Months	13 -15 Months	16 – 18 Months	19 – 21 Months	22- 24 Months
	Source alternative on campus	Switch to Home Learning	Install Tempory Buildings	Install Tempory Buildings	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises

Central Block



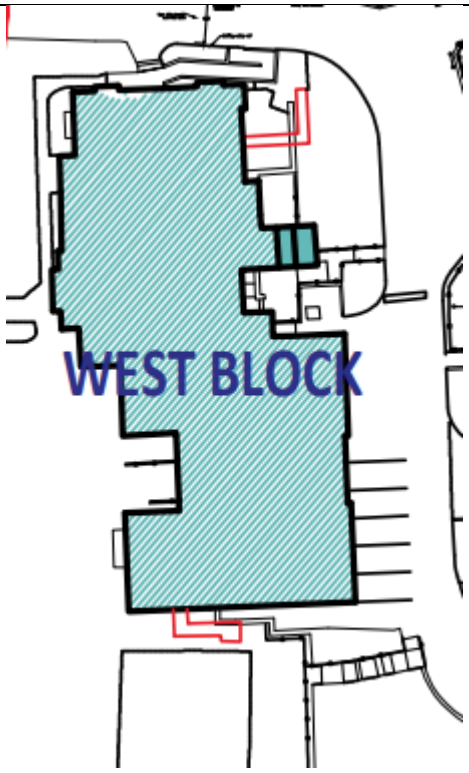
Space Requirement	Month							
	1-3 Months	3 – 6 Months	7 – 9 Months	10 – 12 Months	13 -15 Months	16 – 18 Months	19 – 21 Months	22- 24 Months
	Source alternative on campus	Switch to Home Learning	Install Tempory Buildings	Install Tempory Buildings	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises

North Block 1- 4



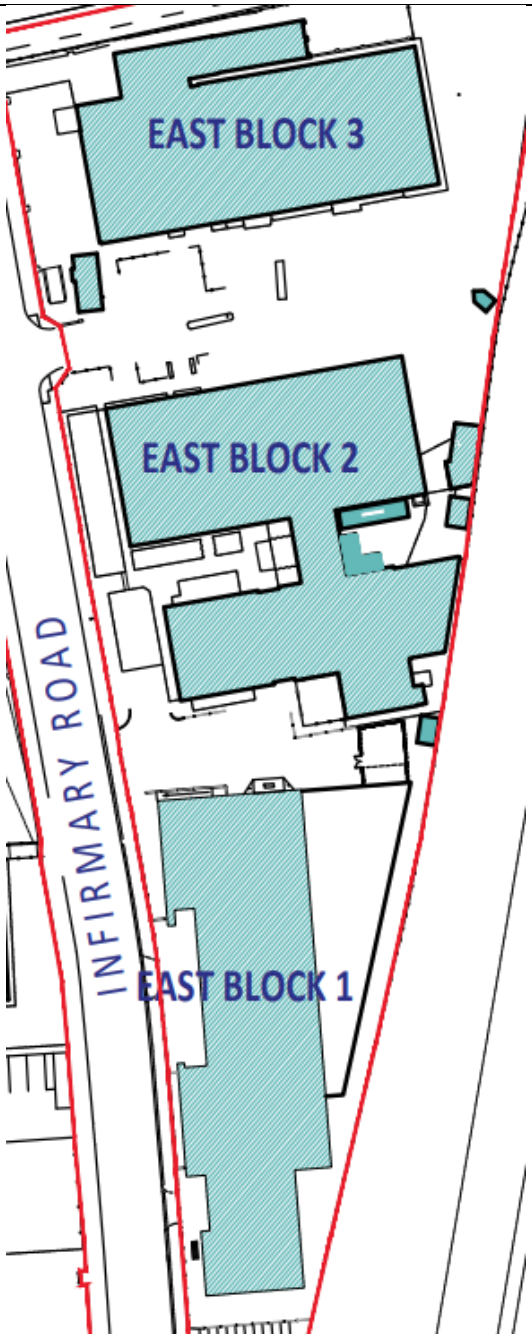
Space Requirement	Month							
	1-3 Months	3 – 6 Months	7 – 9 Months	10 – 12 Months	13 -15 Months	16 – 18 Months	19 – 21 Months	22- 24 Months
	Source alternative on campus	Switch to Home Learning	Install Tempory Buildings	Install Tempory Buildings	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises

West Block



Space Requirement	Month							
	1-3 Months	3 – 6 Months	7 – 9 Months	10 – 12 Months	13 -15 Months	16 – 18 Months	19 – 21 Months	22- 24 Months
	Source alternative on campus	Switch to Home Learning	Install Tempory Buildings	Install Tempory Buildings	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises

East Block 1-3



Space Requirement	Month							
	1-3 Months	3 – 6 Months	7 – 9 Months	10 – 12 Months	13 -15 Months	16 – 18 Months	19 – 21 Months	22- 24 Months
	Source alternative on campus	Switch to Home Learning	Install Tempory Buildings	Install Tempory Buildings	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises	Rent Alternate Premises

Appendix J: ISO22301 Checklist

1. THE ORGANISATION AND ITS CONTEXT	
Have the issues that will drive the BCP been defined?	Yes – Section 8.2
Has the environment within which the BCP will operate (internal & external), and the expected outcomes of the system, been identified?	Yes – Section 3.0
Has an appropriate and repeatable risk assessment method and the acceptable levels of risk been defined and documented?	Yes - Section 8.1

2. NEEDS AND EXPECTATIONS OF INTERESTED PARTIES	
Is the scope of the BCP clear and documented?	Yes – Section 4.0
Is there a procedure in place to identify, consider, document, and maintain information on the applicable legal and regulatory requirements for the BCP?	Yes – Section 6.0
Have these legal, regulatory, and other requirements been communicated to affected employees and identified interested parties?	Yes - Section 7.0

3. SCOPE OF THE BCMS	
Is the scope of the BCP clear and documented?	Yes - Section 4.0
Have options for risk treatment been identified and evaluated?	Yes – Section 8 & 9
Does the scope define the BCMS in terms of its extent, purpose, deliverables, needs and expectations in a way that is appropriate to the organisation?	Yes – Section 4.0
Is there any exclusion from scope, and if so, is it in an area that will not affect the organisation's ability to provide continuity of operations?	N/A

4. LEADERSHIP AND MANAGEMENT COMMITMENT	
Is the organisation's leadership commitment to BCP visible and repeated?	Yes – Section 1.0
Is there a policy, programme, and roles to evidence top management commitment to the BCP?	Yes – Section 7.0
Has top management been appropriately involved in the BCP implementation and review through a formal management review process?	Yes – Section 7 & 1

5. BUSINESS CONTINUITY MANAGEMENT (BCM) POLICY

Is there an established BCP policy that is appropriate, maintained, communicated, and documented?	Yes - Section 5.0
Is the policy available to employees and all interested parties identified?	Yes - Section 1, 5 & 7

6. RISKS AND OPPORTUNITIES OF BCMS IMPLEMENTATION	
Has an analysis of the threats and opportunities that may impact the implementation of the BCP been conducted?	Yes - Section 8 & 9
Has a plan to manage the risks and opportunities of the BCP implementation been developed and actioned?	Yes - Appendices A - H

7. BUSINESS CONTINUITY OBJECTIVES	
Have measurable business continuity (BC) objectives been established, documented, and communicated throughout the organisation?	Yes - Section 5 & 7
Is the achievement of these objectives evaluated by both internal audit and the management review?	Yes – Section 6

8. BCMS RESOURCES AND COMPETENCE	
Are roles within the BCP clearly defined?	Yes - Section 7
Is the BCMS adequately resourced?	Yes -Section 10
Is there a process defined and documented for determining competence for BCP roles?	Yes – Section 7
Are those undertaking BC roles competent, and is this competence documented appropriately?	Yes - Section 7

9. AWARENESS AND COMMUNICATION	
Is everyone within the organisation's control aware of the importance of the BCP policy, their involvement in implementing it and their role in a disruption?	Yes – Sections 6 & 7
Has a communication needs analysis been conducted for the BCP?	Yes – Section 6
Have procedures been confirmed and facilities made available for communicating incidents? Are they regularly tested with results recorded?	Yes - Appendix H
Is appropriate documentation created, maintained, and controlled to demonstrate the effectiveness of the BCPS?	Yes – Sections 6

10. OPERATIONAL PLANNING AND CONTROL

Have you implemented a programme to ensure the BCP achieves its outcomes?	Yes – Section 7
Has there been analysis of the threats to any outsourced processes and their impact on achieving BCP and recovery time objectives?	Yes – Section 7

11. BUSINESS IMPACT ANALYSIS (BIA)	
Is there a formal and documented process for understanding the organisation through a BIA?	Yes – Sections 8 & 9
Is there a formal process for determining continuity objectives based on understanding the impact of disruptive incidents?	Yes – Sections 8 & 9
Does the BIA enable prioritisation of time frames for resuming each activity (Recovery Time Objectives)?	Yes – Sections 8 & 9
Have minimum acceptable levels for resuming activities been identified?	Yes – Sections 8 & 9

12. RISK ASSESSMENT AND TREATMENT	
Is there a formal risk assessment process for analysing the risk of disruptive incidents?	Yes - Section 8
Does this risk assessment method identify risk treatments appropriate to BC objectives?	Yes - Section 8
Is there evidence of prioritising risk treatments with costs identified?	Yes - Section 8

13. BUSINESS CONTINUITY STRATEGY	
Is the BCP strategy based on the outputs of the BIA and risk assessment?	Yes - Section 7 & Appendices A - H
Does the BCP strategy protect prioritised activities and provide appropriate continuity and recovery of them, their dependencies, and resources?	Yes - Section 7 & Appendices A - H
Does the BCP strategy provide for mitigating, responding to and managing impacts?	Yes - Section 7 & Appendices A - H
Have prioritised time frames been set for the resumption of all activities?	Yes - Section 7 & Appendices A - H
Have the BC capabilities of suppliers been evaluated?	Yes - Section 7 & Appendices A - H
Have the resource requirements for the selected strategy options been determined, including people, information and data, infrastructure, facilities, consumables, IT, transport, finance, and supplier services?	Yes - Section 7, 10 & Appendices A – H
Have measures to reduce the likelihood, duration, or impact of a disruption for identified risks been considered and implemented, and are these in accordance with the organisation's risk appetite?	Yes - Section 7 & Appendices A - H

14. ESTABLISHING AND IMPLEMENTING BC PROCEDURES	
Have BCP procedures been put in place to manage a disruptive incident, and have continuity activities based on recovery objectives been identified in the BIA?	Yes -Appendices A - H
Are the business continuity procedures documented?	Yes – Entire Plan
Have internal and external communication protocols been established as part of these procedures?	Yes - Section 6 & 7

15. INCIDENT RESPONSE STRUCTURE (IRS)	
Is there the management structure and trained personnel in place to respond to a disruptive incident?	Yes – Section 7
Does the IRS and associated procedures include thresholds, assessment, activation, resource provision and communication?	Yes – Section 7
Do the people in your IRS have the necessary competency to perform their duties, and have you kept records to demonstrate their competence?	Yes – Section 7

16. INCIDENT COMMUNICATIONS AND WARNINGS	
Is there a procedure for detecting and monitoring incidents?	Yes- Appendices A - H
Is there a procedure for managing internal communications and external communications from interested parties during a disruptive incident?	Yes – Appendix - H
Is there a procedure for receiving and responding to warnings from outside agencies and emergency responders?	Yes - Appendices A – H
Is there a structure to communicate with emergency responders and other authorities during an incident, or in respect of responding organisations, are communications interoperable with others?	Yes – Appendix A – H & Section 7
Is there a procedure for recording vital information about the incident, actions taken, and decisions made?	Yes- Appendices A – H
Is there a procedure for issuing alerts and warnings if appropriate? Are the organisation's communication and warning systems regularly exercised, and records kept of the results?	Yes – Appendix A – H & Section 7
Have measures to reduce the likelihood, duration, or impact of a disruption for identified risks been considered and implemented, and are these in accordance with the organisation's risk appetite?	Yes – Section 9

17. BUSINESS CONTINUITY RESPONSE AND RECOVERY PLANS	
Are there documented plans/procedures for restoring business operations after an incident?	Yes- Appendices A – H
Do these plans reflect the needs of those who will use them?	Yes- Appendices A – H

Do the plans define roles and responsibilities?	Yes – Section 7
Do the plans define a process for activating the response?	Yes Section 7
Do the plans consider the management of the immediate consequences of a disruption, in particular the welfare of individuals, options for response and further loss prevention?	Yes - Section 9
Do the plans detail how to communicate with the various interested parties during the disruption?	Yes - Appendix H
Do the plans contain details on how prioritised activities will be continued or recovered within predetermined time frames?	Yes- Appendices A – H
Is there a planned media response to an incident?	Yes - Appendix H
Do the plans include a procedure for standing down the response?	Yes- Appendices A – H
Does each plan contain the essential information to use it effectively?	Yes- Appendices A – H

18. EXERCISING AND TESTING	
Have business continuity procedures been tested to ensure they are consistent with your BC objectives?	TBA –Procedures in Section 6
Do top management "actively engage" in testing and exercising the BCP?	TBA –Procedures in Section 6
Are the test exercises clearly defined, consistent with the scope of the BCP and business continuity objectives, and based on appropriate scenarios?	TBA –Procedures in Section 6
Will the test exercises that have been conducted over time validate the whole of the organisation's business continuity arrangements?	TBA –Procedures in Section 6
Have formal post-exercise reports been produced for the conducted tests?	TBA –Procedures in Section 6

19. MONITORING, MEASUREMENT, AND EVALUATION	
Has it been determined how (i.e., metrics or KPI's) and when performance of the BCMS will be monitored?	TBA –Procedures in Section 6
Has the performance and effectiveness of the BCP been evaluated and documented, including recordings of any proactive corrective measures taken?	TBA –Procedures in Section 6
Has an appropriate procedure for monitoring the BCP been documented?	TBA –Procedures in Section 6
Are reviews conducted, both periodically and when significant changes occur, to ensure that the business continuity capability is effective and compliant?	TBA –Procedures in Section 6
Are post-incident reviews undertaken and documented following disruptive incidents?	TBA –Procedures in Section 6

20. INTERNAL AUDITS	
Are internal audits conducted periodically to check that the BCP is effective and conforms to both ISO 22301 and the organisation's requirements?	TBA –Procedures in Section 6
Is the audit conducted with an appropriate method, audit programme, and based on the results of risk assessments and previous audits?	TBA –Procedures in Section 6
Are corrective actions implemented and verified without undue delay?	TBA –Procedures in Section 6

21. MANAGEMENT REVIEW	
Do top management undertake a periodic review of the BCP?	Yes – Section 6
Does the management review of the BCP capture the outlined input and output requirements?	Yes – Section 6
Does the output from the BCP management review identify changes and improvements?	Yes – Section 6
Are the results of the management review documented, acted upon, and communicated to appropriate interested parties?	Yes – Section 6

22. CORRECTIVE ACTION AND CONTINUAL IMPROVEMENT	
Have corrective actions for any non-conformities been identified and implemented in the BCP? Is this reported at management review?	TBA –Procedures in Section 6
Do the reviews result in an improvement to the BCMS?	TBA –Procedures in Section 6