

# Business Continuity Plan

## 1. Overview

This plan complements the Critical Incident Policies in place for each school and is referenced within the Trust Risk Assessment. It will be reviewed annually or when significant changes occur.

An emergency is any event which causes, or has the potential to cause, injury, loss of life, damage to property or significant business disruption. Critical Incident Policies are in place to deal with such occurrences.

A disaster is the escalation of an emergency to the point where normal conditions are not expected to be recovered for at least 24 hours. This plan is concerned with the actions required to re-establish operations quickly and efficiently following a disaster. Associated documents include:

- Critical Incident Policies
- Health & Safety Policy and Handbook
- Fire Evacuation Protocols
- First Aid Protocols
- Risk Assessments

Headteachers within the Trust are responsible for operational leadership of the school to which they are assigned. Whilst they are responsible for assessing and declaring emergencies, it is expected that the CEO is fully appraised, and in turn the Chair of Trustees and Chair of the Local Governing Body are informed. Upon potential/actual declaration of a disaster, the Business Continuity Plan will be activated.

## 2. Roles and Responsibilities

The Headteacher will liaise with the CEO regarding any emergency or disaster, and the CFO will be informed.

Led by the Headteacher, the Incident Management Team will comprise the school's SLT members and in addition key colleagues such as site staff where physical buildings are involved, IT staff where ICT services are involved, along with colleagues from central services such as the Central Finance Team Manager and Digital Development Leader as appropriate.

Additional members of the team will be recruited to match the specific needs of the incident. In the event that other staff are sent home, they should remain available during normal working hours to assist with necessary tasks as appropriate.

## 3. Procedure for Closing the School

### ***Closure in advance of a school day***

The school can be closed in advance of a normal school day using the following system:

- a) Closure authorised by the Headteacher, or a Deputy in the absence of the Headteacher. The CEO should be fully informed.
- b) Notification of a school closure using the Local Authority on-line website, linked to radio stations and county website information.
- c) Recording the closure on the home page of the school website.
- d) Sending out text messages to all parents and staff.
- e) Headteacher to alert the Chair of the Local Governing Body and CEO to alert the Chair of Trustees.

### ***Closure during a school day***

It is never a preferred option to close the school during a school day but it can be done using the following procedure:

- a) Closure authorised by the Headteacher, or a Deputy in the absence of the Headteacher. The CEO should be fully informed.
- b) Notification of the school closure using the Local Authority on-line website.
- c) Recording the closure on the home page of the school website.
- d) Contact transport providers to assess collection times.
- e) Sending out text messages to all parents.
- f) Students with parental authorisation may make their way home by themselves.
- g) Students will continue to be supervised by staff until parents authorise them to leave or they are collected.
  - i. Parental authorisation can be provided by text message or email from a parental phone number or email address directly to the student's phone and seen (and recorded) by a member of staff.
  - ii. Consider use of Places of Safety (as described below).
- h) Headteacher to alert Chair of the Local Governing Body, and CEO to alert the Chair of Trustees.
- i) Headteacher to alert other Trust schools, in addition to any other local school as a courtesy.

### ***Off-site place of safety***

If it becomes necessary to evacuate a site completely, students will be escorted to the designated 'place of safety' which is equipped with sufficient facilities such as shelter, toilets and first aid. These are:

- Banovallum School: Queen Elizabeth's Grammar School
- Frithville: Village Hall
- New York: Village Hall
- Queen Elizabeth's Grammar School: Banovallum School

These places also have the space to accommodate the collection of students, either by buses or parents. It will be attempted to secure ICT connectivity and telephone/mobile access via our Digital Development Leader in order to enable emergency communication as required.

## **4. Communication**

After the initial incident, longer term communication to staff will be via the school email system, text messaging or website.

Communication to parents will be via email or text messaging and the school website.

The Headteacher will communicate with the Local Governing Body and the CEO will communicate with the Trust Board, again this is likely to be via email.

## 5. Lockdown Procedure

It is now possible to envisage circumstances where the school may wish to lock itself in, to secure staff and students from an outside threat. This circumstance is described as a 'lockdown'.

If a lockdown is declared:

- In Banovallum, Frithville and QEGS, staff will be advised that 'lockdown' is in operation by audible warning. At New York, where we await replacement alarm systems, this will be via the use of air horns/panic alarms.
- All staff will remain in classrooms and keep students calm and away from windows.
- All students in external PE lessons will be instructed to return inside.
- Registers/roll call will be taken to ensure all students and staff are present.

The lockdown will proceed in the following priority:

- External gates and barriers will be closed and locked.
- External doors will be closed and locked.

Once the site is secure, where CCTV is in place this will be monitored by designated staff (IT staff at secondary schools, administration staff at primary schools). Site staff/key staff will remain positioned as directed by the Headteacher so that doors can be opened quickly if required. Doors, gates and barriers should only be opened when directed by the Headteacher, which will be upon arrival of the Emergency Services or when official confirmation that the threat has passed is received.

## 6. Business Recovery

### ***Insurance***

The nature of requirements will vary according to circumstances. In the first instance contact should be made via the CFO with the school insurers.

### ***Buildings***

If accommodation is required, temporary buildings on existing sites will be the preferred solution. Possible locations for temporary accommodation will depend upon the space and type of base required. In all circumstances, health and safety should be considered in respect of safe evacuation and access for emergency services. When siting temporary buildings, the District Council and our appointed Health & Safety Adviser will be consulted for support and advice.

Should the site be deemed inaccessible for a long period, advice will be sought from the Local Authority, District Council and ESFA regarding suitable alternative arrangements for relocation.

### ***Technology***

School data is held securely, currently this is either upon our own servers, use of Office 365, Google Apps, cloud storage or via Ark ICT Solutions. Data is frequently and routinely backed up as a precaution. Business critical services are determined, in priority order, as follows:

1. Internet and Telephones, including email
2. Student data; SIMS/Integris
3. Sage Financial Software
4. Cashless Catering
5. CCTV
6. Shared/personal drive data
7. Parent Pay online payments

Our ICT staff have the knowledge and experience to act in the event of a disaster in order to establish connectivity as listed above. The top two priorities can be accessed remotely should the whole site be inaccessible, however, power is required to servers to enable remote connectivity. There are two server rooms within the secondary schools, to reduce the risk of failure. During 2019-20 we will be exploring alternative options to mitigate this risk factor further and enhance remote access such as cloud storage as part of the Trust IT Development Plan.

### **Resources**

Where equipment is required, following advice from our insurers, the CFO will support schools via the Central Finance Team to obtain replacement equipment. This may be through reorganisation of Trust resources, short term loan from other educational establishments, hire or purchase as appropriate and will be in accordance with advice received from insurers and our financial procedures.

Where personnel are required, the Headteacher, in conjunction with the CEO, will review the current staffing and deployment, consider options for additional hours or agency staff as appropriate. In the exceptional event of unresolved staff shortage, the timetable may be adjusted to enable quality provision within the constraints of the skills and experience of staff available. Independent study may also be utilised where appropriate and learning resources uploaded to the website.

## **7. Pandemic Threat/Mass Staff Unavailability**

Unavailability of staff is considered a generic threat to operations. The spread of a virus capable of impacting upon operational service delivery is now considered genuine and serious. In the event of mass staff illness or declaration of a pandemic by the authorities, the Headteacher in conjunction with the CEO will close the school using the procedure previously outlined.

## **8. Other Threats**

The following other threats have been considered:

- Buildings unavailable - e.g. fire or flood
- Phone and ICT communications loss
- Finance process breakdown – payments to staff & suppliers fail
- Utilities supply failure
- Key supplier failure - e.g. provisions, transport
- Evacuation due to nearby Incident
- Prolonged bad weather
- Strikes
- Terrorist attack or threat

## Recovery Action Plans

Operational Threat	Steps to Restore Normal Working
<p>A. Building loss – partial or complete (fire, flood, lighting strike etc.)</p>	<ol style="list-style-type: none"> <li>1. Assess site viability for use.</li> <li>2. Liaison with insurers, ESFA and LEA.</li> <li>3. Consider relocation or temporary additional accommodation on site.</li> <li>4. Assess facilities including power, heating, water, toilets, catering.</li> <li>5. Inform suppliers of leased equipment.</li> <li>6. Establish ICT availability on new site including data and communications:               <ul style="list-style-type: none"> <li>• Include consideration of air-conditioned server room with fibre connection, data security and encryption, authentication control for access, back up processes to ensure that we meet electronic and physical data protection obligations.</li> <li>• Purchase required hardware.</li> <li>• Contact suppliers regarding phone lines, cabling and redirecting calls.</li> <li>• Contact supplier for data cabling.</li> <li>• Incorporate phones, email, SIMS/Integris, internet, Sage, Parent Pay.</li> </ul> </li> <li>7. Consider exam schedules and identify alternative centres if relevant. Prioritise access to resources and accommodation for exam students e.g. for revision sessions.</li> <li>8. Identify expected visitors, extracurricular activities, fixtures and lettings and contact them to redirect or cancel as appropriate.</li> <li>9. Ensure communication plan is in place, including parents and transport services.</li> <li>10. Access the Asset Register and assess loss or damage [if lightning strike, consider wiring, data cabling and hardware].</li> <li>11. Consider secure storage for undamaged items whilst the building is replaced/repared, retrieve any accessible resources required for day to day operations.</li> <li>12. Inform suppliers; hold or redirect deliveries and services.</li> <li>13. Procure, through loan/hire/purchase as appropriate, remaining equipment required.</li> <li>14. Rebuild or major refurbishment; project team for design, planning, tender and construction.</li> <li>15. Recovery; site team and appointment of relevant contractors for disposal, deep cleaning, maintenance, decorating and installation of replacement items.</li> </ol>
<p>B. Building denial leading to short term lack of access</p>	<ol style="list-style-type: none"> <li>1. Assess alternative accommodation available or sites which could accommodate temporary classrooms.</li> <li>2. Establish access to ICT.</li> <li>3. Identify resources for independent study, utilise remote access.</li> <li>4. Consider exam schedules and identify alternative centres if relevant. Prioritise access to resources and accommodation for exam students e.g. for revision sessions.</li> <li>5. Ensure communication plan is in place, including parents and transport services.</li> <li>6. Identify expected visitors, extracurricular activities, fixtures and lettings and contact them to redirect or cancel as appropriate.</li> </ol>

Operational Threat	Steps to Restore Normal Working
C. Phone and ICT communications loss	<ol style="list-style-type: none"> <li>1. The main phone systems rely upon electricity to function. Identify any analogue lines which can be used independently, along with mobile phones.</li> <li>2. Where in use, Office 365 and Google Apps will remain accessible, resources can be uploaded for remote working.</li> <li>3. Some primary school data is held locally and relies upon access to the on site server.</li> <li>4. The main servers in secondary schools are protected by battery backup, if this depletes the UPS systems will shut down after approximately 15 minutes. This is to protect against overheating in the server room environment.</li> <li>5. When power is restored, it will take 30-45 minutes for servers to power on and the IT team to check the server room.</li> <li>6. It will then take a further 60 minutes for outlying cabinets and hardware to be checked, including damage to items such as analogue CCTV resulting from power surges.</li> <li>7. Manual registers and roll call records, as located with the CIP, can be used to fulfil our safeguarding obligations until access to SIMS/Integris resumes.</li> <li>8. Should loss be due to theft, in addition to the Police and insurers, consider data security and the need to report to the Information Commissioners Office.</li> </ol>
D. Finance process breakdown – payments to staff & suppliers fail	<ol style="list-style-type: none"> <li>1. Check deadlines, potential penalties and prioritise payments.</li> <li>2. If breakdown is due to ICT, explore access from alternative site.</li> <li>3. If breakdown is due to main bank account issues, consider use of alternative account for urgent payments.</li> <li>4. Alert Lloyds, discuss options/alternative system to on line payments.</li> <li>5. Communicate to relevant parties.</li> </ol>
E. Utilities supply failure	<ol style="list-style-type: none"> <li>1. Check supply points and appliances including activating all emergency shut off switches to ensure site is safe upon reconnection.</li> <li>2. Contact relevant service to establish if the failure is site specific, local area or wider.</li> <li>3. If a date/time of restoration is available, establish the impact upon heating, lighting, resources, toilets, drinking water and catering. Also consider the impact of extremes of weather upon temperatures and site access.</li> <li>4. If the problem is longer term, refer to actions for building denial or loss.</li> <li>5. Ensure communication plan is in place.</li> </ol>
F. Key supplier failure	<ol style="list-style-type: none"> <li>1. Prioritise needs and assess impact on safeguarding, welfare and teaching &amp; learning.</li> <li>2. Establish if supplier has site access and take steps accordingly for site security.</li> <li>3. Establish reason for failure; if financial hold further payments and seek legal advice as appropriate.</li> <li>4. Check existing supplier list, use alternatives where already established.</li> <li>5. Consider sharing resources across Trust school and other education establishments, authorities or businesses.</li> <li>6. Access information for government approved suppliers to seek replacement/bulk supplies e.g. CCS, ESPO, CPC, YPO.</li> <li>7. Consider local suppliers for speed or delivery/smaller quantities.</li> <li>8. If transport is affected, establish a link with the LEA for communications.</li> <li>9. Communicate to parents as appropriate.</li> </ol>

Operational Threat	Steps to Restore Normal Working
G. Evacuation or lockdown due to nearby incident	<ol style="list-style-type: none"> <li>1. Establish estimated duration of incident.</li> <li>2. If prior to school commencing; consider options for closure and follow closure procedure.</li> <li>3. If school is in session; assess likelihood of impact upon transport at the end of the day.</li> <li>4. Communicate to transport services and parents as appropriate.</li> <li>5. Identify expected visitors, extracurricular activities, fixtures and lettings and contact them to cancel.</li> <li>6. Prior to students returning to the site, an inspection should take place to ensure it is safe.</li> <li>7. If school resumes part way during a day, students to return to Form Rooms and registration/roll call should take place to ensure all students and staff are present.</li> </ol>
H. Strikes	<ol style="list-style-type: none"> <li>1. Identify likely impact upon staffing including first aid and catering.</li> <li>2. Identify any specific student groups at risk.</li> <li>3. Identify any planned activities and review the risk assessment e.g. trips.</li> <li>4. If strikes involve emergency services, consider any higher risk activities or events where the strike could impact upon welfare or public safety.</li> <li>5. Consider exam schedules, prioritise exam invigilation, access to resources and accommodation for exam students e.g. for revision sessions.</li> <li>6. If staffing levels result in partial closure, identify resources for independent study, utilise remote access.</li> <li>7. Identify any visitors, extra curricular activities, fixtures and lettings and contact them to cancel as appropriate.</li> <li>8. Ensure communication plan is in place.</li> </ol>
I. Terrorist attack or threat	<ol style="list-style-type: none"> <li>1. If outside of school sessions; prior to students returning to the site, an inspection should take place to ensure it is safe. Refer to building loss or denial section as appropriate.</li> <li>2. If during the school day; students to return to Form Rooms and registration/roll call should take place to ensure all students and staff are present.</li> <li>3. Consider if closure is appropriate.</li> <li>4. Communicate to parents.</li> <li>5. Depending upon the nature of the incident, consider access to support and counselling as noted within the CIP.</li> <li>6. Ensure communication plan is in place.</li> </ol>