



# ADUR & WORTHING C O U N C I L S

## BUSINESS CONTINUITY

### Incident Management Plan PUBLIC / REDACTED VERSION

USE THIS DOCUMENT IN THE EVENT OF A BUSINESS CONTINUITY  
INCIDENT

QUICK ACCESS	
REPORT AN INCIDENT	4
ASSESSMENT OF BUSINESS CONTINUITY LEVEL	6
ACTIVATE THE PLAN	8
ROLES AND RESPONSIBILITIES / ACTION CARDS	16
SUGGESTED STRATEGIES	15
BUSINESS CONTINUITY AGENDA / CHECKLIST	26
RESPONSE GROUP AGENDA / CHECKLIST	28

**Document Control**

<b>Subject</b>	Business Continuity Management
<b>Document</b>	Business Continuity Incident Management Plan <b>Public / Redacted Version</b>
<b>Author</b>	Lloyd Harris - Safety & Resilience Manager, Adur & Worthing Councils <a href="mailto:lloyd.harris@adur-worthing.gov.uk">lloyd.harris@adur-worthing.gov.uk</a> Tel No REDACTED
<b>Primary Reviewers</b>	Adur & Worthing Council Response Group
<b>Version Control</b>	3.2
<b>Last Reviewed</b>	08/07/2025
<b>Review Date</b>	08/07/2028

CONTENTS		
No	Subject	Page
<b>1.0</b>	<b>SECTION 1 INTRODUCTION</b>	
1.1	Purpose	3
1.2	Scope	3
1.3	Authority	3
1.4	Vulnerabilities	4
1.4.1	Introduction	4
1.4.2	Digital	4
1.4.3	Commerce Way	4
1.4.4	Worthing Town Hall / Portland House	4
1.5	Plan Maintenance	4
<b>2.0</b>	<b>SECTION 2 REPORTING AN INCIDENT</b>	<b>4</b>
2.1	Introduction	4
2.2	Report an <b>ICT</b> Incident in office hours	4
2.2.1	Reporting an <b>ICT</b> incident outside of office hours	5
2.3	Reporting <b>all other</b> incidents in Office Hours	5
2.3.1	Reporting <b>all other</b> incidents outside of office hours	5
2.4	Business Continuity Report Form	5
<b>2.5</b>	<b>Reporting Procedure Flow Chart</b>	<b>6</b>
<b>3.0</b>	<b>SECTION 3 RESPONSE LEVEL ASSESSMENT CRITERIA</b>	<b>6</b>
3.1	Assessing a response	6
3.2	Level 1 (Localised) incident criteria	6
3.3	Level 2 (Moderate) incident criteria	7
3.4	Level 3 (Major) incident criteria	7
<b>4.0</b>	<b>SECTION 4 PLAN ACTIVATION</b>	<b>8</b>

4.1	Plan Activation Levels	8
4.2	Level 1 Activation	8
4.3	Level 2 Activation	9
4.4	Level 3 Activation	9
<b>4.5</b>	<b>Activation Procedure Flowchart</b>	<b>9</b>
<b>5.0</b>	<b>SECTION 5 RESPONSE MANAGEMENT</b>	<b>10</b>
5.1	Primary and secondary locations for meetings	10
5.1.1	Alternative locations for meeting	10
5.2	Emergency Control Centre	10
5.3	Communication	11
5.3.1	Contact Information	11
5.3.2	SMS Text Service	11
5.3.3	Teleconferencing / Video conferencing	11
5.3.4	Broadcasting Information to staff using the internet	11
5.3.5	Emergency email address -Email address REDACTED	11
5.3.6	Name of group REDACTED Whatsapp Group Communication Tool	11
5.4	Command Control & Coordination	12
5.5	Impact Assessment (RAG)	12
5.5.1	Frequency of Impact Assessment	12
5.6	Mutual Aid	13
5.6.1	Mutual Aid Requesting Authority	13
5.6.2	Mutual Aid Responding Authority	13
5.6.3	Procedure For Activating Mutual Aid Arrangements	13
5.6.4	Mutual Aid Memorandum of Understanding	13
5.6.5	Memorandum of Understanding Conditions	13
5.7	Informing External Partners	14
5.8	Action Cards (Suggested Strategies)	15
5.9	Finance	15
5.10	Media Enquiries	15
<b>6.0</b>	<b>SECTION 6 ROLES AND RESPONSIBILITIES</b>	<b>15</b>
6.1	Introduction	15
6.2	Response Group	15
6.2.1	Response Group Standing Members	15
6.2.2	Response Group Responsibilities	15
6.3	Assistant Directors	16
6.4	Site Recovery Team	16
<b>7.0</b>	<b>SECTION 7 RECOVERY</b>	<b>17</b>
7.1	Recovery Arrangements	17
7.2	Critical Services - Recovery Time Objectives (RTO)	17
7.3	Critical Services Recovery Point Objectives (RPO)	17
<b>8.0</b>	<b>SECTION 8 TRAINING AND EXERCISING</b>	<b>17</b>
8.1	Business Continuity Platform Training	17
8.2	Exercising	17
	<b>APPENDICES</b>	<b>18</b>
A	Types of Incident & Benchmarks	18

B	Critical Services	21
<b>C</b>	<b>Contact List &amp; Response Group Cascade</b>	<b>23</b>
D	Emergency Email Activation And Instructions	24
E	Response Group Agenda / Checklist (First Meeting)	26
F1	Assistant Director Task List	28
F2	Site Recovery Team Task List	29
F3	Damage Assessment Checklist	31
F4	Insurance Task List	32
F5	Salvage / Asset Protection Task List	33
F6	Alternative Work Area Task List	35
F7	Human Resources / Welfare Task List	37
F8	Health and Safety Task List	38
G1	Loss of Staff Action Card (Suggested Strategies)	39
G2	Damage / Loss of Buildings Action Card (Suggested Strategies)	43
G3	Denial of Fuel / Utilities Action Card (Suggested Strategies)	46
H	Business Continuity Report Form (Manual)	48
I	Impact Assessment (RAG) Form (Manual)	49

## SECTION 1 INTRODUCTION

### 1.1 Purpose

The aim of this document is to provide a framework in which to manage the response of Adur District Council & Worthing Borough Councils to an event which is likely to seriously disrupt the ability to carry out its critical functions. It supports the Adur & Worthing Councils Business Continuity Policy.

### 1.2 Scope

The scope of this document is concerned with the activities of the Councils in the event of a disruptive emergency. It includes guidance for the benefit of the Members and Officers of the Councils.

It complements the Business Impact Assessments and risks to delivery, data contained within the Business Continuity Platform. (MATs)

The plan covers disruption to loss of or denial to Staff, buildings, supplier, vital records and utilities

#### 1.2.1 Out of Scope

This plan does not include I.T Disaster Recovery as this is subject to a separate plan owned by Digital. Any incidents relating to I.T applications disruption, staff should direct their enquiries to Digital.

[Link REDACTED]

### 1.3 Authority

Adur District Council & Worthing Borough Councils are Category 1 responders as defined in Schedule 1: Part 1 (Category 1 Responders: General) of the Civil Contingencies Act 2004, and have duties under that Act. This plan is produced in response to Section 2(1)(c) of the Act.

The Chief Executive of the Councils has overall responsibility for Business Continuity. In the event of an incident, decision making functions are delegated to the Response Group.

## **1.4 Vulnerabilities**

### **1.4.1 Introduction**

Risks identified by the Business Continuity Process have been treated to reduce the probability or impact where possible and within the constraints of control of a given situation. It is not possible to completely remove risks and in the event of a total infrastructure loss, this will present a delayed return to relative normality. This document highlights the risks with a view to ensuring the priority is raised to ensure sufficient resources are committed to resuming business operations as soon as possible.

### **1.4.2 Digital**

ICT operations (Digital) do not provide an out of hours service. With the introduction of cloud based applications such as Google, essential email communication greatly mitigates previous risks allowing users to continue to work from any internet connection. With the introduction of the Cloud Strategy many of the applications have now been transferred to the cloud, mitigating the risk culminating from a loss of the data room. Recent events such as COVID-19 have demonstrated our dynamic ability to mobilise remote working and therefore the reliance on physical office space has been diminished.

### **1.4.3 Commerce Way**

Commerce Way houses specialist equipment and assets which are not duplicated elsewhere. A building loss may have significant impacts and delays in the recovery of the services and functions operating from this site. Mutual aid agreements may also be necessary in the short term to share facilities with neighbouring authorities.

### **1.4.3 Worthing Town Hall**

The main administrative building of the council is Worthing Town Hall. A denial of access to this building would result in an element of disruption. Remote working is now the established norm; it would depend on the continued access and operation of the server room for some software and network connectivity. Alternative smaller accommodation is available which can be utilised to provide working areas in the short to medium term.

For long term accommodation needs, the authority will consider taking over the Shoreham Centre as an office space.

## **1.5 Plan Maintenance**

This plan will be reviewed every three years by the Safety & Resilience Team or following an incident requiring coordination by the aforementioned.

## **SECTION 2**

### **2.0 REPORTING AN INCIDENT**

#### **2.1 Introduction**

The reporting of incidents is dependent upon the type of incident and time of incident. These can be placed into two categories. ICT and Non related ICT issues. ICT system failure can hinder reporting procedures so it is important that all reports are reported as soon as possible.

#### **2.2 Reporting An ICT Incident In Office Hours**

If it is possible, log the call by emailing [email REDACTED] or if this fails phone [Tel No REDACTED]

### **2.2.1 Reporting An ICT incident Outside Of Office Hours**

There is no out of hours service for Digital. This decision is based on the fact that no critical systems are used outside of the normal working hours and therefore the risk is low. If incidents indicate significant disruption to systems employees should report the matter as per 2.3.1. This is for the Incident Manager to assess and escalate as required.

### **2.3 Reporting all other incidents in Office Hours**

Serious incidents can be reported to the Response Group via the Safety & Resilience Team in [LINK REDACTED]

Minor incidents may be reported using the Business Continuity report form as soon as reasonably practicable.

Go to [Link REDACTED]

### **2.3.1 Reporting all other incidents outside of office hours**

If an incident occurs outside of core working hours the Out of Hours Service must be called immediately quoting "Business Continuity Incident" and request the Incident Manager is informed. The Incident Manager will assess the incident and possible activation of this plan as well as the service business continuity information located on the MATs platform. [LINK REDACTED]

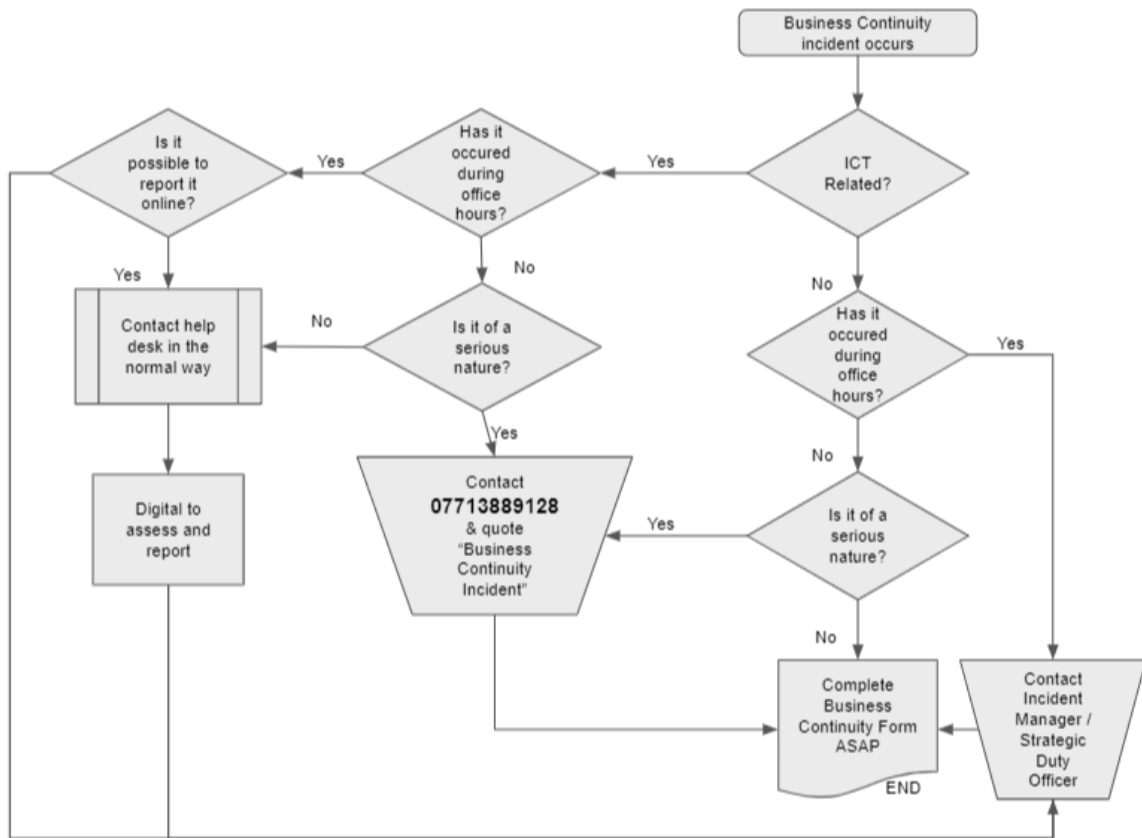
### **2.4 Business Continuity Report Form**

A Business Continuity Report form has been created on Google Forms which is used to report any incidents affecting the organisation. All responses are emailed directly to the Response Group via [Email address REDACTED] for assessment.

Go to [Intranet Link [REDACTED]]

The data is compiled on a Google sheet contained within the Business Continuity folder on Google Drive. A manual copy of the form is stored on Google Drive for printing as required. (See [APPENDIX H](#))

## 2.5 Reporting Procedure Flowchart



## SECTION 3

### 3.0 RESPONSE LEVEL ASSESSMENT CRITERIA (TRIGGERS)

**3.1 Assessing a Response** is sometimes difficult to confidently assess the impact of an incident as all the information will not be immediately available. Time lost during a response can never be regained. It is always better to convene a response early on in the process and subsequently stand it down if it is not required rather than missing an opportunity to contain the incident and prevent escalation.

This plan is activated based upon three levels of disruption which is dependent on the type and severity of incident. Some examples of types in incident and versus level of response can be found at [APPENDIX A](#).

### 3.2 LEVEL 1 - (LOCALISED) INCIDENT CRITERIA

Defined as not being an emergency and does not cause serious threat of disruption to people, premises and critical functions services. Consequences are likely to be limited disruption to a singular service and pose no threat to the reputation of the Authority. Normal and routine service contingencies should suffice to rectify issues. Any prolonged exposure of a disruption will need to be monitored by service managers and escalation to level 2 should be considered if there is prolonged disruption to critical services or it becomes a reputational issue.

### **3.3 LEVEL 2 - (MODERATE) INCIDENT CRITERIA**

This is defined as an incident that could pose an actual threat to people, premises and critical services over a length of time, but not seriously affecting the overall functioning of the Authority. Examples may include a temporary reduction in staff, medium term loss to an ICT system and communications, temporary short term loss of utilities or temporary short term evacuation of a premises. This may involve the Emergency Services. Incidents that have potential legal ramifications or threaten the reputation of the Authority should also be considered.

### **3.4 LEVEL 3 (MAJOR) INCIDENT CRITERIA**

This is defined as an incident causing a significant disruption to the Authority's operations. It may affect an entire building or a number of buildings, employees or visitors, with the escalation potential to require the intervention of the Emergency Services who are likely to take operational control of the incident, at least in the initial stages. Assistance from other Local Authorities under the mutual aid agreement may be a serious consideration to maintain critical services.

The benchmark for considering a level three is to consider whether the incident falls into the category of an emergency as defined by the Civil Contingency Act or major incident which affects a local regional or national geographic area.

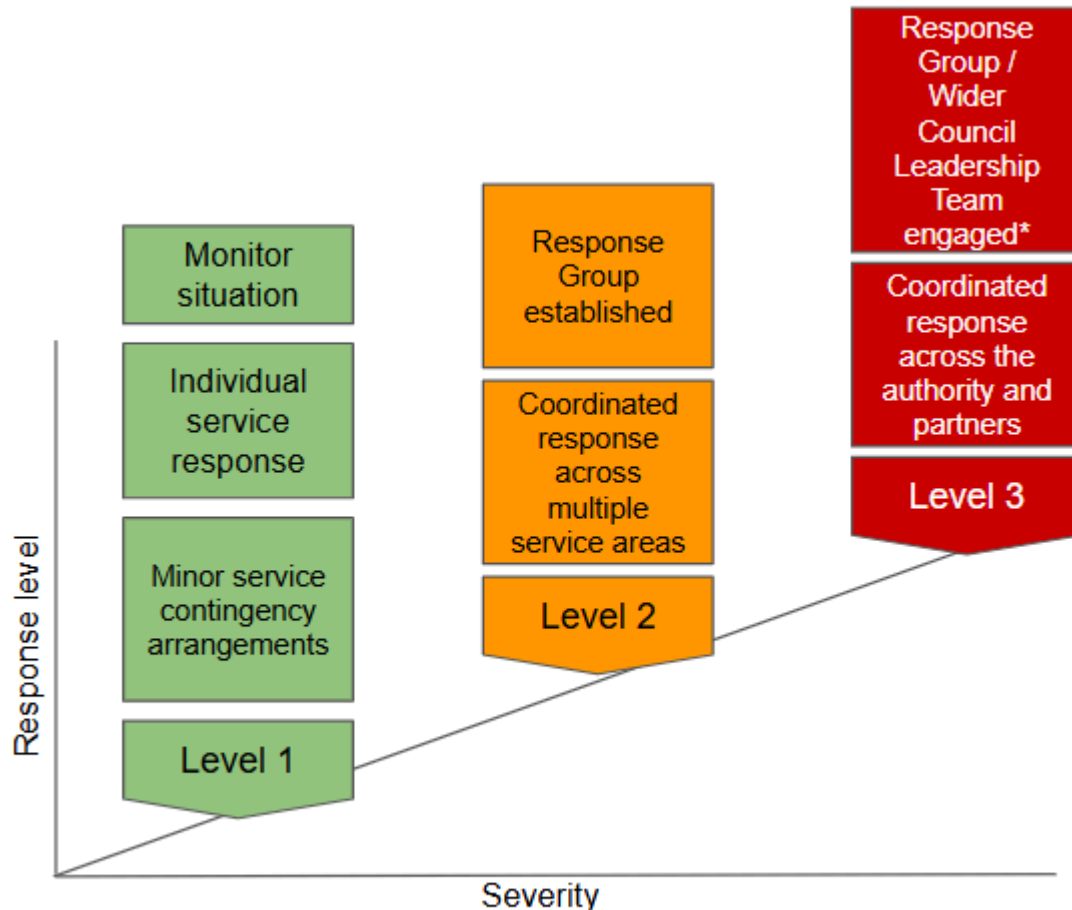


## SECTION 4

### 4.0 PLAN ACTIVATION

#### 4.1 Plan Activation

The Business Continuity Incident Management Plan and associated service Business Continuity Plans will be activated to provide the most appropriate framework in order to manage and coordinate the incident in accordance with need.



\* At the discretion of the Chief Executive

#### 4.2 LEVEL 1 Activation

Service managers should invoke their own business continuity plan located on the Business Continuity Platform and report contingency arrangements to their Assistant Director / Head of Service. The Safety & Resilience Team will monitor the situation and escalate to level 2 if required. There is not normally a requirement to coordinate a meeting **unless** there is a likelihood that that the situation will escalate or become prolonged.

If a level 1 incident is reported outside of office hours, the Incident Manager will record the incident and assess the situation in consultation with the Strategic Duty Officer.

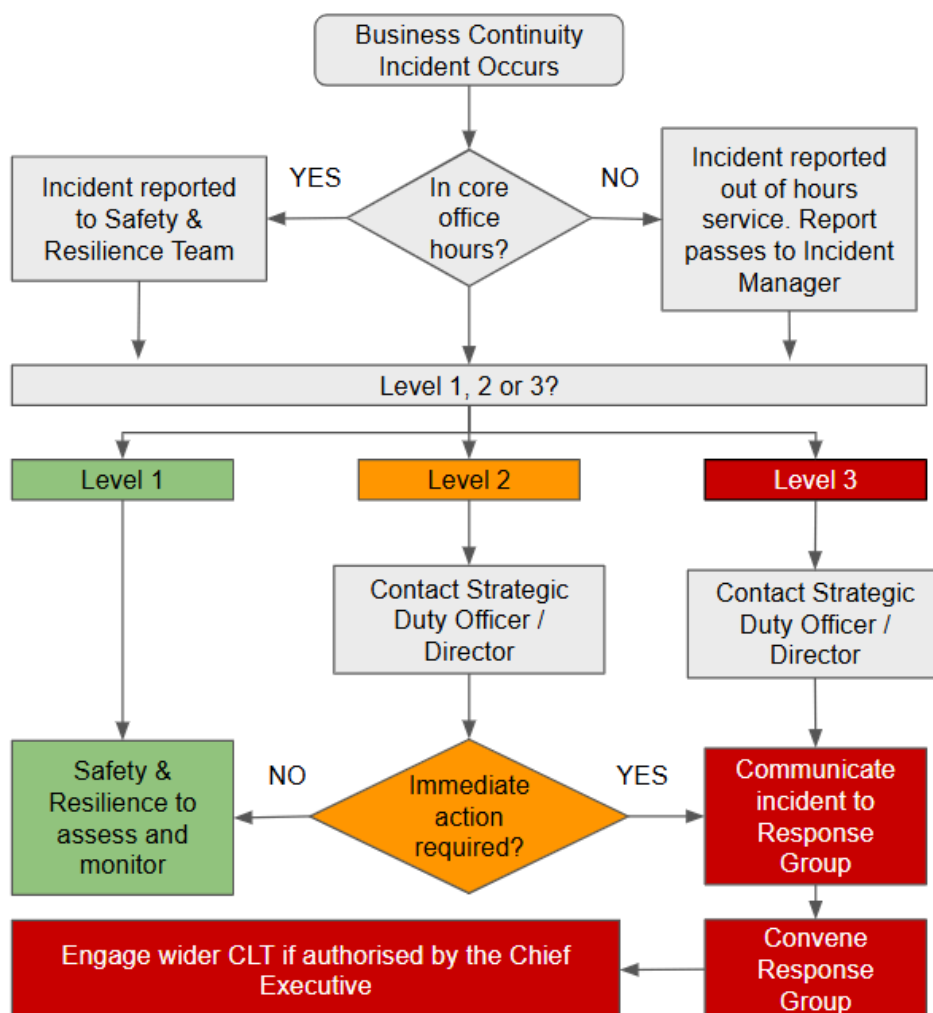
### 4.3 LEVEL 2 Activation

The Response Group will activate the Business Continuity Incident Management Plan and convene as soon as possible to coordinate the response.

### 4.4 LEVEL 3 Activation

This is the same for LEVEL 2 with the additional escalation of informing the wider Council Leadership Team (CLT) at the discretion of the Chief Executive. It may be considered satisfactory to maintain the coordinated response in the Response Group depending on the type of incident.

### 4.5 Activation Procedure Flowchart



The activation will differ according to the severity of the incident and time of day. The preferred method to communicate an incident to the Response Group is to use the SMS text service; however, any suitable method may be employed.

For LEVEL 3 incidents it is imperative that a meeting of the Response Group is convened as soon as possible regardless of the time of day. An initial teleconference / video conference can be accommodated to organise a suitable location should a physical meeting be necessary.

## SECTION 5

### 5.0 RESPONSE MANAGEMENT

#### 5.1 Primary And Secondary Locations For Meetings

The primary course of action for convening a meeting should always be video teleconferencing unless the incident makes this impossible. The rationale is that the virtual meeting can be convened quickly and negates the requirement for unnecessary travel.

During core office hours the default location for holding response Group meetings is [Location REDACTED] (if required). If there is difficulty in finding an appropriate room within a time critical period, representatives should meet outside [Location REDACTED]. Precedence must be given over other routine meetings to accommodate this group.

Primary	Secondary
Location REDACTED	Location REDACTED
Out of Hours Access	
Call the Out of Hours Service on 07713889128 and ask for the "Incident Manager"	

##### 5.1.1 Alternative Locations For Meetings

In the event of an area wide evacuation the following remote locations are suitable for meetings.

Facility	Access out of hours
Location REDACTED	Call the Out of Hours Service on 07713 889128 and ask for the "Incident Manager"
Location REDACTED	
Location REDACTED	

#### 5.2 Emergency Control Centre Function

Current thinking is that a physical Emergency Control Centre is not required as there are suitable I.T solutions to be able to work collaboratively remotely using a number of different methods;

- Zoom Video conferencing
- Google Meet
- Incident Log to record actions, decisions and rationale

## **5.3 Communication**

### **5.3.1 Contact Information**

Contact information is contained within the Duty Officer Roster on the Google Calendar. It lists the duty officers for the day.

An 'Emergency Response Contact List' is also available via the Safety and Resilience Team / Incident Manager and also accessible to authorised users via the Emergency Response Folder on Google Drive. (Folder - "Internal Contact List") See [Appendix REDACTED].

### **5.3.2 SMS Text Service**

Instructions for transmitting an SMS Text can be found at  
[Link REDACTED]

### **5.3.3 Teleconferencing / Video Conferencing**

Unless otherwise directed, the Incident Manager / Strategic Duty Officer will convene the first tele/video meeting using Google Meet.

### **5.3.4 Broadcasting Information To Staff Using The Internet**

There is a page attached to the Adur & Worthing website which can be activated to provide information to staff. In order to use this facility the page must be switched on. The page is not protected by a password and therefore sensitive information must not be conveyed. For instructions [Link REDACTED] or go to the Emergency Response Folder >> Procedures >> 3 Emergency Web Page

### **5.3.5 Emergency Email Address**

The Safety and Resilience Team will determine whether the emergency email address will be activated.

The following email address should be used to collate information and respond to enquiries during a level 2 / 3 incident.

[Email address REDACTED]

[Appendix REDACTED]

This allows for staff involved in a business continuity incident to receive all email correspondence in one location. Individual users are able to reply using the email address.

The Response Group has access to this inbox. Digital can add additional staff on request up to a maximum of 25 staff.

If emails are sent to individual staff the email should be forwarded to the emergency email address so it can be reviewed by incident staff and respond accordingly.

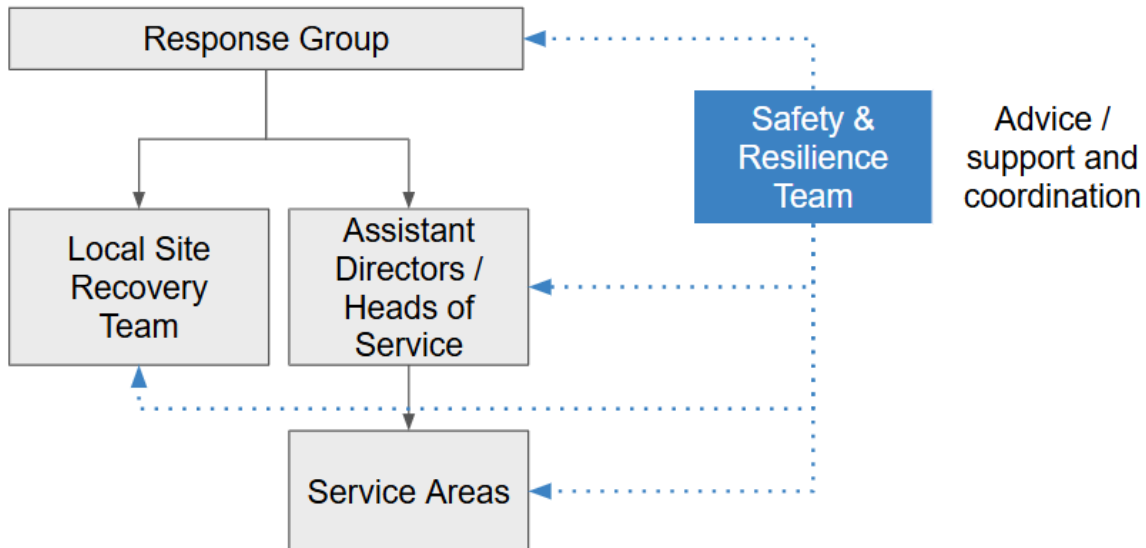
All staff should be encouraged to use this address if and when required.

### **5.3.6 [Group name REDACTED] Whatsapp Group Communication Tool**

A Whatsapp group called [Group name REDACTED] has been set up to allow fast communication to key officers and provide updates in real time. The Safety and Resilience Team administers this group.

## 5.4 Command, Control & Coordination

The following organisation chart illustrates the command control and coordination of a business continuity incident.



## 5.5 Impact Assessment (RAG)

It is important early on in any process to determine the current status of the organisation. The Response Group will instruct Service managers to report their level of capability. Assistant Directors are ultimately responsible for ensuring impact assessments are completed and submitted within the requested time frame.

The information to be completed via the Intranet or a link to a cloud based form. In the event of a total ICT failure manual copies can be distributed. See [APPENDIX I](#).

This request will enable the Response Group to assess the following information.

Highlight any deficiencies in the key areas such as people, premises, information, ICT and suppliers

- Clarify the specific issues affecting a service.
- Identify current resources available to maintain critical services.
- Identify any spare capacity to assist with any other critical services.
- Actions taken to recover from the incident.
- Requests for assistance to maintain critical services.

Each service will be able to indicate the current level of capability using a traffic light system which works in parallel with the activation levels documented in this plan.

### 5.5.1 Frequency of Impact Assessment

The frequency for information requests will be determined by the Response Group.

## **5.6 Mutual Aid**

An agreement between Category 1 and 2 responders and other organisations not covered by the Act, within the same sector or across sectors and across boundaries to provide assistance with additional resources during an emergency, which may overwhelm the resources of an individual organisation.

### **5.6.1 Mutual Aid Requesting Authority**

Any local authority in need of assistance during the management of an emergency. They will be liable for negligent acts committed by any staff while so loaned and should ensure that there is adequate employer's liability insurance in place in respect of them.

### **5.6.2 Mutual Aid Responding Authority**

Any local authority supplying resources to a requesting Authority during an emergency.

### **5.6.3 Procedure For Activating Mutual Aid Arrangements**

The Chief Executive or any officer acting on his or her behalf may make a request to the Chief Executive or any other officer acting on his or her behalf of any other local authority asking for assistance, such request to be formalised in writing if so required by either party.

The mutual aid requested could include staff for all or any of the following functions:-

- Emergency Planning Officers
- Environmental Health
- Engineers
- Building Control / Structural Engineering
- Local Authority Emergency Control Centres
- Emergency Assistance Centres
- Beach Cleansing
- Family Liaison Team
- Such other purposes as may prove to be useful

The mutual aid requested might also take the form of the Responding Authority releasing a contractor from routine obligations in order to provide additional support to a Requesting Authority.

Equipment loaned to the requesting authority will:

- Be covered by the requesting authority
- Return any equipment in the same order as when received
- Replace and disposable items used

### **5.6.4 Mutual Aid Memorandum of Understanding**

The provision of mutual aid has been agreed by all unitary, county and district & borough councils in East and West Sussex. (as per the mutual aid agreement held by the Safety and Resilience Team)

### **5.6.5 Memorandum of Understanding Conditions**

A formal request for aid shall only be made by a Chief Executive or designated lead officer with the authority of the Chief Executive to a Chief Executive / designated lead.

A Chief Executive / designated lead who receives a request for assistance shall take the appropriate action to respond to the request without delay and, in the case of a lead officer, shall inform the Chief Executive at the earliest opportunity. As part of the decision process, the Chief Executive of the Responding Authority must consider whether the resource requested can be made available without putting at risk the authority's service delivery obligations or ability to respond to an emergency of its own.

The Responding Authority undertakes, so far as is reasonably practicable, to provide suitable staff for the task to be performed.

Responsibility for coordinating aid for meeting all legal requirements for the supervision, training and health and safety of loaned staff rests with the Requesting Authority or, where more than one authority area has been affected by the emergency, by the authority that requested the aid with whom the relevant staff are principally assisting.

A Requesting Authority shall bear the financial costs associated with the provision of aid, and shall reimburse the Responding Authority on a cost recovery basis upon the termination of the aid and within a reasonable period of time following the receipt of a fully documented statement from the Responding Authority.

All of the authorities named in the Memorandum of Understanding shall maintain adequate insurance arrangements to cover mutual aid circumstances and any liabilities arising from the deployment of staff from and to another authority area.

The Responding Authority should make arrangements to ensure that regular contact is maintained with its staff working for the Requesting Authority and ensure that management issues are dealt with appropriately. The Chief Executives or lead officers of the Responding Authority and Requesting Authority should maintain regular contact throughout the loan period.

Any disputes between the Responding and Requesting Authorities should be resolved through negotiations between the lead officers or Chief Executives with a view to early resolution. An unresolved dispute should be referred to an independent Chief Executive, that is the Chief Executive of an authority named in the mutual aid agreement but uninvolved in the emergency, or if all named authorities are involved, then the Chief Executive of an authority which is not a party to the agreement who shall suggest a solution to the dispute within 14 days of the referral.

The Memorandum of Understanding is not intended to be a legally binding contract.

## 5.7 Informing External Partners

Where a business continuity incident affects the wider community e.g. severe weather, all responding partners as part of the Sussex Resilience Forum (SRF) are requested to provide an update of the organisation's ability to operate as part of the wider monitoring process. This enables a commonly reported information picture to be created in order to create a partnership response.

The Safety & Resilience Team will be responsible for providing the information based on the level of business continuity incident.

Adur & Worthing Councils will report the status to reflect the Sussex RAG assessment commonly known as the Sussex Common Reported Information Picture (SCRIP).

Adur & Worthing Councils Status	Sussex Resilience Forum Assessment
LEVEL 1	GREEN
LEVEL 2	AMBER
LEVEL 3	RED

## **5.8 Action Cards (Suggested Strategies)**

This plan provides a number of task lists for coordinators to consider in managing and reducing the impacts of an incident.

Loss of Staff - See [APPENDIX G1](#)

Damage / Loss of Building - See [APPENDIX G2](#)

Denial of Fuel / Utilities - See [APPENDIX G3](#)

## **5.9 Finance**

Financial Services will be responsible for providing a cost code for the incident. There are a number of corporate credit holders in the council that can purchase emergency supplies. Finance can provide details.

## **5.10 Media Enquiries**

The Assistant Director for People and Change is responsible for developing a media response during a business continuity incident. All media enquiries must be referred to the Response Group immediately. If media representatives arrive at an affected location, do not provide any statements until full consultation with the Response Group, Incident Manager or Assistant Director of People and Change..

# **SECTION 6**

## **6.0 ROLES AND RESPONSIBILITIES**

### **6.1 Introduction**

The following Roles and Responsibilities will vary according to the type of incident and demands required to recover from the event. Membership to groups has to remain flexible to allow the required skill sets and affected Assistant Directors to attend.

### **6.2 Response Group**

See [APPENDIX E](#) for meeting agenda and checklist

#### **6.2.1 Standing Members**

Standing Members will be dependent on the type of incident and affected areas. It may be restricted to a minority or in respect of a Level 3 incident, all of the Council Leadership Team will likely be required to attend in addition to key officers. The arrangements for activation of this group are identical to the Emergency Plan.

#### **6.2.2 Response Group Responsibilities**

- Monitor and continually assess the impacts on a local incident.
- Be prepared to take over overall coordination if the situation escalates or the incident is beyond the capabilities of the service affected.
- Provide overall coordination and a flexible framework for incident response to ensure agreed critical functions are maintained at an agreed level.
- Agree and set up collaborative working arrangements (remotely or physical)
- Ensure the welfare, safety and security of staff and customers.
- Restore services to relative or agreed relative normality in the shortest time scale possible.
- communicate effectively and proactively, before, during and after incidents with internal and external stakeholders.



### 6.3 Assistant Directors

See [APPENDIX F1](#) for task list

- Manage LEVEL 1 incidents using service Business Continuity Plans and normal and routine service planning.
- Activate business continuity arrangements for each service under their responsibility
- Monitor and assess the impacts of the incident.
- Escalate any prolonged or complex incidents to the Response Group / Response Group.
- Support the Response Group in delivering an effective response.
- Report service capability (RAG Assessment) to the Safety & Resilience Team when requested.
- Attend Business Continuity Response Group meetings If the assistant director is not available, provide a suitable and competent substitute.
- Provide information to all staff under their responsibility on a frequent basis.
- Assume responsibility for the health and safety of staff under their responsibility.
- Appoint a Site Recovery Team from existing staff to recover information and assets.

### 6.4 Site Recovery Team

See [APPENDIX F2](#) for task list

If an incident has occurred involving the destruction or damage to a building or assets, there may well be a need for a salvage operation to take place. It is essential that the plan identifies the location of important documents within the site on the site plan. The Fire and Rescue Service are the lead emergency service on salvage matters during the incident and in the immediate aftermath.

Information about the whereabouts of key documents will help them prioritise their salvage efforts. However, in the longer term, directorates and/or other organisations may be in a better position to assist.

The recovery and safe-keeping of documents will be of major concern and it may be necessary to let this aspect of the recovery process be dealt with by experts from specialist document recovery firms. These specialists employ measures such as air drying and vacuum freezing to stop any further damage occurring to documents whilst measures are taken to recover either the document or the information they contained. Contacting a specialist recovery firm quickly is very important.

The Salvage Team will in the first instance be competent officers who have responsibility for the day to day running of the affected building. In the absence of a suitable officer, the most senior officer on site will assign the task until permanent arrangements can be made.

The following tasks will be assigned to carry out this function.

- Site Recovery Team - See [APPENDIX F2](#)
- Damage Assessment Officer - Building Control Officer. See [APPENDIX F3](#)
- Insurance Officer. See [APPENDIX F4](#)
- Salvage/Asset Protection Officer - Facilities Officer. See [APPENDIX F5](#)
- Alternative Work Area Officer - See [APPENDIX F6](#)
- HR / Welfare Officer - See [APPENDIX F7](#)
- Health & Safety Officer (Safety & Resilience) - See [APPENDIX F8](#)

## SECTION 7

### 7.0 RECOVERY

#### 7.1. Recovery Arrangements

Recovery is the term used to describe the restoration of a situation back to relative and agreed “new” normality. Soon after the incident occurs early consideration should be given to establishing a recovery sub group to examine the longer term issues which will need to be managed in order to establish an acceptable level of business operations. Depending on the severity of the incident it may never be possible to restore business to exactly the way it was before. The Response Group should agree on a level that the organisation is happy with to stand down the response.

Assistance on recovery can be found by referring to the Sussex Resilience Forum Recovery Plan which is available via the Safety & Resilience Team or via the Emergency Response Folder on Google Drive.

#### 7.2 Critical Services - Recovery Time Objectives (RTO)

Recovery will depend on the type of incident and who it affects individual service areas. Each service area can have a number of constituent parts namely business units, as reflected on the Business Continuity Application. For the purposes of this plan, a strategic approach has been adopted to provide a suggested indication of what services need to take priority and in what order. The recovery time objective (RTO) data may differ from this plan for a number of reasons, however, managers of service areas should consult and work towards their own recovery, based upon their business impact assessments unless otherwise directed by the Response Group. The restoration of critical services will be governed and reviewed by the Response Group to consider additional resources and solutions. The priorities may change over time.

See [APPENDIX B](#) for an indicative list of critical services and intended recovery times

#### 7.3 Critical Services Recovery Point Objectives (RPO)

Critical Services relating to Recovery Point Objectives are subject to Disaster Recovery arising from an ICT incident. Users should refer to this plan for further information.

[Link REDACTED]

The Recovery Point Objective is defined as “The goal for how fast to restore technology services after a disruption (based on the acceptable amount of downtime and level of performance). For example, a recovery time objective of 24 hours with local accessibility for payroll services means that the payroll application must be up and running within 24 hours as well as accessible locally.”

## SECTION 8

### 8.0 TRAINING & EXERCISING

#### 8.1 Business Continuity Platform Training

Training is offered on a one to one basis, relevant to the needs of the service area and business units. The Safety & Resilience Team aims to monitor the business unit within the organisation subject to organisational redesigns and attempts to offer training when the need arises. This training is complemented with a reference training manual for new and existing users.

#### 8.2 Exercising

A senior level exercise is scheduled for a minimum of every three years to test this plan in conjunction with emergency planning exercises, using emergency / business continuity scenarios. This is attended by the Council Leadership Team. Exercises are restricted to desktop scenarios due to limited resources available.

## APPENDIX A

## TYPES OF INCIDENT &amp; BENCHMARKS

Type of Incident	Level 1 (Local)	Level 2 (Moderate)	Level 3 (Major)
<b>Building damage / destruction</b>	Minor structural damage. No evacuation necessary.	Minor structural damage. Evacuation and limited relocation likely	Total building loss, Rebuild, significant repair. Full evacuation and relocation necessary.
<b>Adverse Weather</b>	Some staff absences, Travel restrictions.Minor effects to premises. Minor short term disruption to normal services	Significant staff reduction. Building damage requiring temporary suspension of operations.	Serious building damage. Serious disruption to critical services. Significant staff reduction. Relocation necessary.
<b>Fires</b>	No relocation necessary. Little or no information loss. Rooms temporarily unavailable.	Medium damage, loss of some accommodation. Can reorganise internally to continue. Loss of information	Major damage to the council's infrastructure. Long term relocation necessary. Significant information loss.
<b>Flooding</b>	Minor damage to rooms / minimal water egress. No loss of critical equipment or documents. Little or no disruption. Minor staff absence / redeployment	Medium damage to rooms and equipment. Some loss or damage to documents / information storage. Remedial work and relocation necessary. Significant staff reduction / redeployment.	Major damage to rooms, equipment and information sources. Serious disruption to facilities and infrastructure.
<b>Civil Disorder</b>	Minor and temporary disruption to normal services. Minor staff absence.	Serious disruption to critical services. Significant staff reduction. Travel restriction. Premises unsafe to use	Serious prolonged disruption. Multi Agency Emergency Declared. Critical Services significantly impaired.
<b>Utility failure more than one day</b>	Little or no disruption	Unable to sustain ICT. Heating / Water not available. Multi Agency response in place. Temporary loss of premises.	Sustained utility failure to premises. No electric / water / heating /fuel for prolonged time. Staff unable to use premises. Multi agency response in place
<b>Explosions</b>	Small localised blast - Can be isolated. No effects on council business	Blast affects buildings. Increased security. No toxic release. Some staff are absent. No specific threat against	Significant damage to buildings. Terrorism threat raised. Council specific threat from terrorism. Significant staff absence.

		council or targeted campaigns	Critical functions severely disrupted.
<b>Gas Leaks</b>	Minor leak in building. Short term evacuation required.	Major leak in buildings or adjacent to. Evacuation required.	Prolonged disruption to council services
<b>Bomb Threat</b>	Suspicious parcel. Isolated incident. No specific intelligence or threats.	Viable device found Sustained threats, hate campaigns targeted against councils. Police involved	Prolonged disruption to council services
<b>Health Epidemics</b>	Minor short term staff absence. Implement Health advice Encourage remote working to prevent spread.	Local community spread Moderate and manageable disruption to critical services. Low to medium staff absence. Defined health procedures implemented.	Widespread infection affecting large areas of the country. Central Government Coordination / Strategy  Workforce isolation through mass remote working  Use of premises for inoculation / medical triage
<b>Adverse public interest</b>	Interest by local press only	Significant local press interest requiring coordinated response	Regional, National press interest. Coordinated response and additional resources required.
<b>ICT failure / disruption</b>	Temporary loss or disruption affected 5-10% of the councils. Recovery expected within 1-2 days.	Loss or disruption affecting critical processes and time related activity. Recovery not expected within 48 hours. Minimal reputational damage.	Large scale system failure. The majority of councils' critical services are severely disrupted. Reputational damage. Income loss. Benefits not paid.
<b>Death of employees or multiple serious injuries</b>		1 death. Local press interest. Regulatory investigation. Possible prosecution.	Multiple deaths or injuries. Regulatory / criminal investigation. Significant adverse media interest. Prosecution possible.
<b>Industrial Action</b>	Work to rule internally. Small picket lines. Minor disruption to services. External action resulting in minor staff absence. Travel restrictions	Significant staff absence through strikes by internal staff or external organisations for 1 day Significant disruption to services	Prolonged industrial action affecting the majority of council services. Significant staff absence. Essential external services affecting safety and wellbeing of community and staff.
<b>Multi Agency Emergency (CCA 2004)</b>	Minimal disruption to critical services. No changes in working practices. Localised incident	Supporting role to emergency services. Deployment of staff to assist. Short term	A wide area emergency is declared. The community is adversely affected. Large scale evacuation. Prolonged displacement of

		<p>evacuation in the community.</p> <p>Short term displacement of persons.</p> <p>Wide ranging incident</p> <p>Some staff absence / redeployment</p>	<p>persons. Significant council resources redeployment.</p> <p>Suspension of services.</p>
--	--	--	--

## APPENDIX B

<b>CRITICAL SERVICES</b>
--------------------------

FOR ICT related incidents refer to the [Link REDACTED] for recovery point objectives  
THIS IS A STRATEGIC INDICATION FOR RECOVERY PURPOSES

Service Impact	Recovery Time Objective
<b>HIGH</b>	
Safety & Resilience	Continuous
Facilities	1 day
Housing Homelessness	1 day
Media (communications)	2 days
Waste Services Domestic	2 days
Environmental Health Public Health	2 days
Legal Services	3 days
Crematorium and Cemeteries	3 days
<b>MEDIUM</b>	
Help point / customer services	3-5 days
Building Control	3-5 days
Housing repairs	5 days
Waste Service - Trade / Commercial	5 days
ICT Servers / Telephony	5 days
Council Tax	5 days
Public Health and Regulation - Inspections	5 days
Health & Safety	5 days
Insurance	5 days
Finance (including payroll)	5 days
<b>LOW</b>	

Records and Admin	7 days
Planning	7 days
Parks & Foreshores	7 days
Direct services – repairs	7 days
ICT generally	7 days
Waste Services – Recycling	7 days
Policy and Strategy	10 days
Electoral Services	10 days (depending on election dates)
Democratic Services	10 days

**APPENDIX C**

**CONTACT LIST & Response Group CASCADE**

To Activate the Business Continuity Incident Management Plan

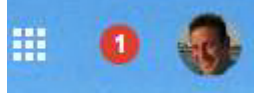







[REDACTED]

**Response Group Contact List**

[REDACTED]



APPENDIX D

EMERGENCY EMAIL ACTIVATION AND INSTRUCTIONS		
1	In Gmail click on your personal email profile icon located in the top right hand corner	
2	Available users should click on the Emergency inbox to access the inbox. If you do not see the inbox contact a Response Group representative who will contact ICT urgently and request access. Up to 25 users may be assigned to this inbox.  IT request made 12:38 08/07/2016 Ref IM102186	[Image REDACTED]
3	All incoming emails will be labelled AWAITING to identify those that need progressing. Work in time order if there are excessive amounts of emails. Once an enquiry has been started remove and apply the IN PROGRESS label (See below)	
4	If an email is urgent apply the label URGENT. A filter has been created to apply a label if URGENT appears anywhere in the message. Urgent should only be used if the enquiry is of a time critical nature or poses a threat to life or property. If urgent no longer applies remove the label to avoid confusion.	
5	Apply the IN PROGRESS email when the email has been seen and actions have completed however, it is not in a position to be closed	
6	When an enquiry has been completed remove all other labels and apply a CLOSED label. It is beneficial to end the email conversation by forwarding to [Email address REDACTED] with a brief explanation of the reason for closure. This assists the reviewing process. Example - FWD to [Email address REDACTED] <a href="#">Subject - Keep the same subject</a> <a href="#">Message - Enquiry closed as telephones are now working.</a> <a href="#">Information received from Andrew James. No further actions outstanding. Agreed by P Brewer</a>	
7	Apply a Tactical Label when a decision is required on the enquiry by a representative of the Response Group. Both the IN PROGRESS and TACTICAL labels should be present. Remove the TACTICAL label when it no longer applies.	
8	Apply a Strategic Label when a decision is required on the enquiry by a representative of the Emergency Management Team. Both the IN PROGRESS and STRATEGIC labels should be present. Remove the STRATEGIC label when it no longer applies.	
	Apply an <b>**OVERDUE**</b> label when the enquiry has not received the necessary response. This review process should be undertaken regularly by an officer responsible for managing the Emergency Control Centre.	

	The label should be removed once the appropriate response has been received and the enquiry is on track.	
9	Additional labels may be established in accordance with local arrangements.	
10	If an email comes from a person outside the organisation be sure to add this to the contacts for future use. Locate the sender on the right hand side of the message and click on the down arrow next to the envelope icon. Select "Add to Contacts"	
11	A digital signature has been set up and will be sent as a reply to all incoming emails. <b>IMPORTANT - ONCE A TELEPHONE NUMBER AND EMERGENCY CONTROL CENTRE IS ESTABLISHED ENTER THE DETAILS INTO THE DIGITAL SIGNATURE.</b>  Go to the cog on the top right hand side and select "Settings" In the General tab scroll down until you come to the signature option. Enter the required information and select Save Changes at the bottom of the screen	
12	The Out of Office reply is switched on by default to provide information to other users.	

## APPENDIX E

RESPONSE GROUP AGENDA / CHECKLIST (FIRST MEETING)		
1	Agree on Chair (If Director not available)	
2	Confirm Business Continuity incident level (1,2 or 3) (See Section 3)	
3	Emergency issues - Issues that pose a risk to life or property	
4	<b>Situation Report</b> What has happened? (What do we know as fact?) Location / Service / Function affected Number of staff / buildings / services / functions Length of time disruption is anticipated.	
5	Staff deployment considerations	
6	Service suspension / reduction	
7	Allocate Tasks (Appendices F1 to F8) as appropriate	
8	Communications with internal / external stakeholders.	
9	Recovery working group consideration (Lead / staffing / purpose / location)	
10	Establish 'battle rhythm' for meetings, data collection i.e. RAG assessments etc	
11	Complete Checklist	
RESPONSE GROUP CHECKLIST		Y/N
A	Commence a log (If possible use Google Docs)	
B	Does the Group require additional members to make decisions?	
C	Is a "runner" required to pass messages or distribute equipment	
D	Has a single point of contact been established for further reporting?	
E	Have Service Business Continuity Plans been activated?	
F	Consider informing remaining CLT members to establish the Emergency Management Team?	
G	Use the emergency mailbox to coordinate the incident? [Email address REDACTED] or use existing methods?	
H	Activate web page [Email address REDACTED] ? (to alert staff of updates when not connected to the council network)	
I	Request Impact Assessment (RAG) to be completed to obtain an accurate picture of disruption? Set frequency	
J	Building Loss / Damage - Confirm initial Site Recovery Team has been established by a CLT officer. Appoint specialist staff for the role?	
K	Building Loss / Damage - Investigate alternative work areas?	
L	Is there a requirement to reduce / suspend services?	
M	Is there a requirement to redeploy staff / encourage home working?	

N	Do we need external assistance (Mutual aid / external contractors / hire of equipment?)	
O	Develop media strategy to inform key stakeholders. Manage the narrative.	
P	Agree on frequency and content for broadcasting to staff. (Where to go / What to do / Who to call.)	
Q	Arrange for cost code to be established for use to manage the incident?	
R	Formulation of a recovery team to be established to look at longer term issues?	
S	Do shifts need to be considered to continue management of the incident. (Send staff home for rest?)	
T	Establish frequency of meetings	

## APPENDIX F1

ASSISTANT DIRECTOR TASK LIST		
<p>The following tasks are suggestions and may not be applied in all circumstances. All tasks must be considered and any decision NOT to proceed must be documented</p> <p><b>If activated send all correspondence / enquiries to [Email address REDACTED otherwise use [Email address REDACTED]</b></p>		
No	Activity	Comments
1	Ensure incident reports are submitted to the Response Group / ICT	See Reporting an incident
2	Add actions to the incident log covering actions taken, tasks delegated and decisions made.	
3	Activate Service Business Continuity Plans	
4	Inform staff as soon possible with clear concise instructions	If activated, staff may use the internet web page [Email address REDACTED] to receive updates on the current situation. All requests to place information on this page must go through the Response Group. Do not reveal this web page to any outside the organisation.
5	Convene a meeting with service managers as soon as possible to discuss impacts and gather all available information.	
6	Assess the impact of the Business Continuity Incident with a view to completing the RAG assessment if required.	See Impact Assessment (RAG)
7	Loss of Buildings Appoint an interim Site Recovery Team to liaise with emergency services. This function will be superseded by specialist staff once decided by the Response Group	
8	Assume responsibility for the health and safety of staff	
9	Appoint a single point of contact for communication and instructions	
10	Prepare to attend the Response Group or Emergency Control Centre if requested	See Mutual Aid
11	Send communications relating to the incident to [Email address REDACTED]	
12	Refer to Incident Task lists in this plan for strategies for managing the incident.	

## APPENDIX F2

SITE RECOVERY TEAM TASK LIST		
<p>The following tasks are suggestions and may not be applied in all circumstances. All tasks must be considered and any decision NOT to proceed must be documented.</p> <p><b>Send all correspondence / enquiries to</b> [Email address REDACTED] <b>and</b> [Email address REDACTED]</p>		
No	Activity	Comments
1	Assemble Site Recovery Team from available staff.	In the interim this may be organised locally by a Head of Service. The Head of Service will appoint a single point of contact for this temporary team. The <b>Response Group</b> to appoint suitable specialist staff as soon as possible.
2	Start an incident log covering actions taken, task delegated and decisions made (or add to existing log)	
3	Consider appointing the following key staff Damage Assessment Officer Insurance Officer Salvage / Asset Protection Officer Alternative Work Area Officer HR Officer Health & Safety Officer	<p>Task lists are provided for each role.</p> <p>Transport coordination needs will be the responsibility of the <b>Alternative Work Area Officer</b>.</p>
4	Confirm the Alternative Work Area requirements	<p>Confirm with the <b>Alternative Work Area Officer</b> that the predetermined facilities for each section / team at the alternative work area are in place.</p> <ul style="list-style-type: none"> <li>• This should be a case of confirming your resource requirements.</li> <li>• Flag any items no longer required.</li> <li>• You might be able to request additional facilities at this stage.</li> <li>• Prepare an inventory containing information regarding the facilities requirements of each department.</li> </ul>
5	Review which vital records need to be retrieved.	This will include backup data tapes etc. kept off site.
6	If you have any LANs, Desktops or Mid-range systems that need recovering, contact Digital for assistance.	
7	Be advised of when the alternative work area can be occupied by the teams.	<p>You will be notified when the alternative work area is ready for occupation by the <b>Alternative Work Area Officer</b>.</p> <p>No team will be allowed to relocate without the approval of the Response Group.</p>
8	Verify new work area	<p>Check that the office facilities with which you have been provided, agree with those requested and / or pre-arranged. In particular:-</p> <ul style="list-style-type: none"> <li>• Health and Safety Assessment</li> <li>• Check Telephones works as expected and have the correct extensions allocated.</li> <li>• Check special stationery is available.</li> <li>• Any other requirements</li> </ul>

9	Organise the Department	Organise the work area so that restoration and resumption of the key tasks can commence in an orderly way.
10	Coordinate replacement assets	Coordinate furniture / equipment deliveries to the alternative work area with the <b>Alternative Work Area Officer</b>
11	Restore Back Ups	ICT will recover all LAN servers and provide technical assistance for the provision of information Technology services. Advise the <b>Response Group</b> of any problems associated with the recovery of back-up information.
12	Obtain replacement ICT equipment	Advise the <b>Response Group</b> of the need to obtain essential emergency replacement PC Hardware or software to provide recovery that is not provided by a DR contract.
13	Confirm stationery and office supply requirements	Review stationery and office supply requirements and forward replacement requests to the <b>Alternative Work Area Officer</b> .
14	Notify important contacts	Confirm with the <b>Response Group</b> who has been notified of the situation in broad terms at a high level. Contact:- <ul style="list-style-type: none"> <li>• Non critical suppliers</li> <li>• Regulatory Authorities</li> <li>• Key Clients, agents, services.</li> <li>• Staff at other sites who are dealt with on a regular basis. Reassure that they will soon be dealt with as normally as possible and give some indication as to when this will be.</li> <li>• Report to the <b>Response Group</b> if it is felt that any important contacts have not been informed of the situation at a high enough level.</li> </ul>
15	Check the status of mainframe mid-range LAN, WAN etc. and communication links, as appropriate.	Once informed that ICT services are available, have the teams test that these have been properly restored, in particular: The applications work as expected The data appears to be correct at the point in time to which it should have been recovered. Printers and any special connections work normally. Check the output as is expected e.g. from overnight runs for the days missed since the incident is delivered and appears to be correct.. Establish status and availability of telecommunications links, both voice and data. Consider redirection of telephone calls if appropriate.
16	Perform Key Tasks	The services the teams provide are limited to the key tasks as defined unless the Response Group indicates otherwise. Prioritise these tasks and arrange for their completion on a normal basis as possible

## APPENDIX F3

DAMAGE ASSESSMENT TASK LIST			
<p><b>(To be completed by the Damage Assessment Officer)</b></p> <p>Please note that staff are not to place themselves or others at risk by carrying out the building damage assessment. This is a specialised area and will be carried out by a specialist either from or arranged through Building Control or Surveyors.</p> <p><b>If activated send all correspondence / enquiries to</b> [Email address REDACTED] <b>cc</b> [Email address REDACTED]</p>			
Area checked	Damage Assessment	Date / Time Checked	Signature
Building Structure			
<b>Services</b>			
Power			
Lighting			
Heating			
Water supply			
Plumbing			
Fire Alarms			
Other			
Computer systems and networks			
Telecoms equipment			
Office equipment and assets			

Upon completion submit to the **Response Group**



## APPENDIX F4

INSURANCE TASK LIST		
<p><b>(To be handed to the person designated to lead the completion of any insurance claim on behalf of the Council.)</b></p> <p>This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.</p> <p style="text-align: center;"><b>Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the Response Group.</b></p> <p>Please refer any questions or uncertainty to the Response Group as they are responsible for managing and coordinating the incident.</p> <p>For your information, claims amounting to £50,000 or under are self insured, but a Loss Adjuster may be appointed by Risk Management.</p> <p>Risk Management will also have contacts of companies that can provide assistance in the restoration and storage of salvaged materials.</p>		
No	Activity	Comments
1	Set up activity log covering actions taken, tasks delegated and decisions made.	Preferably use existing incident log to record actions. The Safety & Resilience Team can provide access.
2	Log all expenditure	Obtain cost codes from Financial Services
3	Liaise with Risk Management for all activity regarding; <ul style="list-style-type: none"> <li>• Property</li> <li>• Insurers</li> <li>• Legal</li> <li>• Appointment of Loss Adjuster</li> </ul>	
4	Keep the Response Group informed.	
5	Assist in the completion of any insurance claim.	
6	Be aware that staff or others in the building at the time of the incident may incur personal losses.	These may not be insured through their own policies.
7	If a salvage area has been set up, work with the team present at the location to report all salvaged assets.	

## APPENDIX F5

SALVAGE / ASSET PROTECTION TASK LIST		
<p>(To be handed to the person designated to lead the salvage of damaged property from the building)</p> <p>This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.</p> <p><b>Under no circumstances should contact be made with any media organisation.</b></p> <p>Please refer any requests for media contact to the Response Group</p> <p>Please refer any questions or uncertainty to the Business Recovery Team as they are responsible for managing and coordinating the incident.</p> <p>For your information, claims amounting to £50,000 or under are self insured, but a Loss Adjuster may be appointed..</p>		
No	Activity	Comments
1	Set up an incident log covering actions taken, tasks delegated and decisions made.	
2	Log all expenditure and submit logs periodically to the Financial Administrator.	
3	Locate an area of suitable size e.g. spare office, warehouse, etc. to which everything removed from the building can initially be taken for assessment and checking.	This should be reasonably close to the incident site but outside any cordoned off area. Secure and provide adequate fire protection. Consider consulting with the Facilities Officer
4	For ease of identification when assets are removed, colour code incident building into areas by floor, phase or logical grouping. Use same coding at the receiving salvage area so that when assets are received there they can be placed into the same area.	For example, assets removed from the second floor should be placed in the receiving area designated as the second floor.
5	Set aside an area within the receiving salvage area for the receiving of salvaged papers and items which may have been blown from the building and retrieved from the street or surrounding area	
6	Obtain full asset register listing from the affected business functions of all assets normally in their part of the building.	
7	Set up a procedure to log the removal of all assets from incident building to receiving salvage area. As assets are removed, security should check that removal of assets is authorised, by whom and where they are being taken and signed out.	Note: pedestal desks should not be locked but taped securely with warehouse type tape as there is a tendency for keys to become separated.
8	Priority should be given to the removal of all personal belongings from the incident building e.g. handbags, coats, wallets, keys etc. Ensure all such items removed are bagged in clear plastic bags and have a sticker on them warning that they may be contaminated, contain glass pieces etc. (depending on incident).	Priority salvage should be for staff related assets and business critical assets. Liaise with Risk Manager for Loss Adjuster contact.

9	Keep the Response Group informed.	
10	Arrange for any vehicles within the building perimeter to be moved to a designated motor dealership or agent.	Vehicles may be part of the company fleet or employee owned.
11	Arrange for all equipment to be checked by a specialist company for possible contamination by carbon deposits.	<p>This includes all electronic equipment and PC medium e.g. CD ROM, PC floppy disks etc.</p> <p>No unchecked equipment or medium must be taken for use at any alternative work area centres without being certified as checked and OK to use.</p>

#### Consideration for equipment damage following explosion

1. Initial shock wave damage to silicon, glass components and enclosed devices is not always apparent. May look outwardly undamaged.
2. Risk of implosion from VDUs requires careful handling.
3. All identified key equipment to be cocooned to prevent further deterioration.
4. Keyboards may not be cost effective to salvage.
5. Dumb terminals and VDUs with damage to casings and scratched screens may not be worth salvaging.
6. All system units to be salvaged with attempted recovery of data.
7. Low expectation of equipment and re-use.
8. Catalogue all system units by asset number, processor chip, memory and size of hard disk to assist in claim.
9. Any salvaged disks to be expertly copied to new disk before use to prevent contamination and damage.

## APPENDIX F6

ALTERNATIVE WORK AREA TASK LIST		
No	Activity	Comment
1	The <b>Response Group</b> will advise which alternative work areas are to be used.	Liaise with the <b>Response Group</b> for their Critical Business Services, <b>Alternative Work Areas</b> and timescales.
2	Set up your own activity log covering actions taken, tasks delegated and decisions made.	
3	Contact the provider of the <b>alternative work area(s)</b> and put on standby or invoke use of the centre, depending on whether final assessment of incident and impact on business has been made.	The alternative work areas may be within existing buildings or supplied by a third party.
4	Assign task lists to others as appropriate for activity in preparing the facilities and services at the <b>alternative work areas</b> : <ul style="list-style-type: none"> <li>• Human Resources</li> <li>• Welfare</li> <li>• Health and Safety</li> </ul>	
5	Co-opt others as required to achieve this function.	
6	Log all expenditure	Obtain cost codes from Financial Services
7	Ascertain from the Business unit(s) / teams numbers of staff expected to move to <b>alternative work areas</b> and at what times.	
8	Liaise with the providers of the <b>alternative work areas</b> to ensure all predefined equipment and furniture is in place as per requirements.	
9	Liaise with <b>alternative work areas</b> facilities personnel regarding: <ul style="list-style-type: none"> <li>• Level of security provided for both staff and building.</li> <li>• The provision of office cleaning services including the removal of rubbish and confidential waste.</li> </ul>	Establish procedure for identification and access of staff both daytime and out-of hours.
10	Ensure minimum number of photocopiers are operational and check arrangements for supplies of paper, toner, etc. including maintenance and breakdown.	Liaise with Procurement Services
11	Set up stationery cupboard supplies for the normal usage items and make arrangements for ordering non-standard items.	
12	Set up Post Room facility to mirror as closely as possible messenger service previously provided.	Liaise with Business Support to carry out this function
13	Prepare a welcome booklet for all arriving staff giving details of health and safety provision, emergency procedures, first aid, post and messenger services, general administration etc.	Safety & Resilience and Building Control can assist with this function.
14	Set up shredder(s) or means of securely holding confidential waste paper until removal.	
15	In conjunction with alternative work areas, facilities personnel, arrange for an evacuation test using a fire alarm system within one week of staff occupying the building.	

16	Designate an area for the receiving of records, disks, equipment etc. either from vital records or salvaged from the incident site via the salvage location, before allowing it to pass out to the relevant business unit/team.	
17	Notify suppliers of known regular deliveries of new sites and details.	Existing regular orders may need to be amended.

## APPENDIX F7

HUMAN RESOURCES / WELFARE TASK LIST		
<p><b>(To be handed to the person designated to lead on Human Resources and Welfare)</b></p> <p>This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.</p> <p><b>Under no circumstances should contact be made with any media organisation.</b></p> <p>Please refer any requests for media contact to the <b>Response Group</b>.</p> <p>Please refer any questions or uncertainty to the <b>Response Group</b> as they are responsible for managing and coordinating the incident.</p>		
1	Set up activity log covering actions taken, tasks delegated and decisions made.	Use the master log sheet set up by Safety & Resilience Team
2	Log all expenditure.	Obtain cost codes from Financial Services
3	Update the <b>Response Group</b> frequently	
4	Establish from the business unit(s) which alternative work areas are being used and numbers of staff expecting to be at the new locations and in what timescales.	For lack of staff consideration may have to be given to contacting local temporary employment agencies.
5	Liaise with pre-defined transport providers to set up arrangements for transporting staff to new locations.	Consider pick up points, frequency of service, opportunity for park and ride, out-of hours working, use of public transport etc.
6	Avoid bringing in too many staff on site at the same time in the initial occupancy period at the alternative work areas.	Only bring people in who can be gainfully employed. Ideally they should be phased in by department or team. This allows some settling in before the next team arrives.
7	Oversee working hours expected of staff to ensure that adequate rest periods are taken or enforced.	
8	Provide a separate area where debriefing and counselling can take place in private.	This may be away from the site.
9	Confirm provision for catering, both drinks vending and meals and what is/can be provided on site / off site for daytime and out of-hours working.	Consider drinks vending machines on free vend to help staff settle in.
10	Agree with Human Resources department criteria and payment calculations for staff who relocate in terms of travelling costs, overtime etc.	
11	Check personnel records to ensure all employee information is up-to-date including home telephone numbers	
12	Assist the <b>Site Recovery Team</b> to prepare and provide daily briefing progress update to staff not working at the alternative work areas but asked to either work from home or just stay at home.	

## APPENDIX F8

HEALTH AND SAFETY TASK LIST		
<p>(To be handed to the person designated to lead on Health and Safety at the Alternative Work areas)</p> <p>This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.</p> <p><b>Under no circumstances should contact be made with any media organisation.</b></p> <p>Please refer any requests for media contact to the <b>Response Group</b>.</p> <p>Please refer any questions or uncertainty to the <b>Response Group</b> as they are responsible for managing and coordinating the incident.</p>		
1	Set up own activity log covering actions taken, tasks delegated and decisions made.	Where tasks are delegated, include review time.
2	Do not have any discussions with the media – this is a specialist and sensitive area.	Refer any media enquiries to the <b>Response Group</b> .
3	Establish the maximum number of persons that can be present on site as stipulated on the Fire Risk Assessment.	Ensure this figure is not exceeded.
4	Check that the premises have the minimum and correct requirements for fire signs, extinguishers, fire blankets etc.	
5	Log all expenditure.	Obtain cost codes from Financial Services.
6	Establish First Aid provision if First Aid facilities are not provided.	First Aid may be provided by on site security team or it may be necessary to set up first aid boxes and a First Aid roster.
7	Issue DSE assessment to all personnel using workstations.	Provide remedial equipment e.g. footrests, wrist rests, copy holders etc. where identified.
8	Locate accident book.	
9	Consider whether a COSHH assessment needs to be undertaken.	There should already be one in the building as a whole unless it has been an unoccupied building.
10	Despite the attractiveness, do not allow staff to bring in any portable electrical equipment from home UNLESS it can be tested by a qualified electrician for Portable Appliance Testing (this should only be used for the minimum period only).	Ask to see Portable Appliance Testing logs for all equipment provided at the <b>alternative work areas</b> .
11	If necessary, appoint a Health and Safety Representative.	
12	Prepare, with others, an emergency evacuation procedure for all building occupants and carry out an evacuation test using a fire alarm system within one week of staff occupying the building.	
13	Set up enough Emergency Marshals to cover all areas of the alternative work areas occupied by staff.	Briefing sessions with new Emergency Marshals could help them become familiar with the layout and escape routes of the newly occupied building.

## APPENDIX G1

LOSS OF STAFF ACTION CARD (Suggested Strategies)		
Key Threat	Potential Triggers	Risk Width
Loss of specialist staff	Flu / Pandemic, Severe Weather, Industrial Action Large scale disaster Road Gridlock Fuel crisis.	All services and staff
Risk Strategies		
<p>Threat Strategies:</p> <ol style="list-style-type: none"> <li>1. Work longer hours in initial phase</li> <li>2. Move staff internally</li> <li>3. Home working</li> <li>4. Reciprocal agreements with other LAs</li> <li>5. Agency staff</li> </ol> <p>All critical services will consider strategies 1-3 as part of the immediate response with options 4 and 5 being considered to cover medium or long term.</p>		
Actions To Maintain Service		Timing
Convene the <b>Response Group</b> (Immediately if a sudden incident such as severe weather or when agreed trigger point is reached for 'rising tide' event such as pandemic flu). Trigger point is when first case of flu is reported in Adur & Worthing Councils		<24 hrs
Assess the actual/potential loss of staff and distribution of losses across directorates using RAG assessment reporting form.		<24 hrs
Assess the duration of likely staff loss. Manage absence reporting (for flu) and maintain a log of team staff levels.		<24 hrs
<p>Identify the minimum service levels for the critical services that apply (i.e. that should be recovered) during the incident.</p> <p>Identify those less critical services that can be scaled down or stopped.</p> <p>Identify how long reduced service standards can be enforced before becoming critical before issues such as staff or service user welfare occur.</p> <p>Identify any statutory implications for relaxed standards or scaled down services.</p> <p>Be aware of irregular but time critical events such as elections.</p>		<24 hrs
Maintain a log of where staff are located to and who has changed their work pattern		<24 hrs
<p>Identify the skill gap – i.e. the shortfall between the staff (and their skills) available and those required to maintain critical services</p> <p>Review the alternatives for closing that gap, see below.</p>		<24 hrs



Devise and activate communications strategy to advise key stakeholders	<24 hrs	Comms
Open discussions with trade union representatives on temporary changes to T&C and any enabling support that is required.	<24 hrs	People and Change / Unions
Identify any additional support services required to enable staff to focus on service provision e.g. counselling, food on site, flexible working, childcare etc.	<24 hrs	People and Change / Unions
<b>1. Work Longer / Different Hours</b>		
Assess the potential - i.e. staff (and their appropriate skills) who are willing and able and whose family arrangements allow them to work longer hours	<24 hrs	Assistant Directors
Consider shorter or alternative work times for staff that have home responsibilities (i.e. schools closed).	<24 hrs	Assistant Directors
Make sure H&S is maintained i.e. heating is on, security of building is maintained.	As appropriate	Response Group / Facilities
Contact the relevant staff to confirm their availability and provide instructions on what to do / where to go via e-mail, telephone, SMS or web page <a href="#">[Email address REDACTED]</a> (See Communications)	<24 hrs	Safety & Resilience / Digital
Brief all other staff on changes to working arrangements	<24 hrs	Comms
Monitor situation/effectiveness of actions taken, stand down arrangements when necessary.	As appropriate	Response Group / Assistant Directors
<b>2. Internal Staff Movement</b>		
Identify and assess the staff gaps (numbers / length of time /skills / requirements) - Use RAG assessment form	<24 hrs	Response Group / Assistant Directors
Contact relevant staff who are to be redeployed and confirm the willingness and ability to be redeployed by e-mail, telephone or text message. Agree with line managers.	<24 hrs	Response Group / People and Change / Assistant Directors
Manage/support the redeployment staff, i.e. provide an induction/briefing/instruction, provide any relevant procedures or standard practices and assess the risk associated with redeployment to critical or sensitive roles. Plus their health and safety.	<24 hrs	Service managers
Monitor situation/effectiveness of actions taken, stand down arrangements when necessary.	As appropriate	Response Group
<b>3. Home Working</b>		
NOTE - This option is most appropriate for; <ul style="list-style-type: none"> <li>Flu Pandemic or contagious diseases (reduces risk of infection)</li> <li>Severe weather.</li> </ul>		
Identify staff who are already working remotely (e.g. severe weather) using RAG assessment. Identify and contact staff who should work remotely (e.g. flu pandemic). Using RAG assessment.	<24 hrs by 1000 of working day	Assistant Directors
Check the sustainability of expected home working levels, i.e. the IT	<24 hrs	Response

requirements		Group/ Digital
Contact relevant staff via e-mail, telephone or text message.	<24 hrs	Assistant Director / Service manager
Activate and use <a href="#">[Email address REDACTED]</a> webpage to maintain communications with remote staff	<24 hrs	Safety & Resilience / RG / Intranet administrators
Monitor situation / stand down remote working when crisis passed	<24 hrs	Assistant Directors
<b>4. Mutual Aid Agreement with Local Authorities</b>		
Identify and assess either the staff gaps (numbers/length of time/skills requirements) or the service/work that needs to be maintained/done.	2 - 3 days	Response Group / Assistant Directors
Seek authority from CLT to approach and discuss mutual aid with other local authorities	2 - 3 days	Response Group
Consider redirection of calls to another provider.	2 - 3 days	Digital / Customer Services
Set up new temporary number / script to redirect calls or seek information on website	2 - 3 days	Digital / Customer Services
Authorise additional expenditure to fund arrangements	2 - 3 days	Finance
<b>5. Agency Staff</b>		
Note – this option is not relevant to Flu pandemic, as all agencies will also be incapacitated.		
Identify/assess the staff gaps;- numbers, length of time and skill requirements.	2 - 3 days	Assistant Directors
Identify and contact the relevant agency for the staff/skills required.	2 - 3 days	Assistant Directors
Notify the insurance company when agency staff are employed.		Insurance Manager
Authorise expenditure on staffing	>3 days	Finance
Manage/support the new staff, there is a process for new staff induction i.e. provide an induction/briefing/instruction, provide any relevant procedures or standard practices, assess the risk associated with agency staff to critical or sensitive roles. Check what limits and authorisation levels exist for agency staff at management posts.	>3 days	Assistant Directors
Monitor effectiveness of actions, stand down deployment when crisis passed.	As appropriate	Response Group / Assistant Directors
<b>Retired or Voluntary Staff</b>		
NOTE - There is no formal process for this option.		
Ask members to help out where applicable	> 1 week	CLT

Identify/assess the staff gaps that may be filled by people who have appropriate skills/experience within local communities who may be retired/unemployed professionals.	2 - 3 days	Response Group
Identify how such people may be made aware, i.e. local media broadcasts.	2 - 3 days	Head of Comms
On receipt of a significant number of volunteers, discuss the process for recruitment with HR.	2 -3 days	Response Group
Seek guidance from insurance company	2 - 3 days	Insurance Officer

## APPENDIX G2

DAMAGE / LOSS OF BUILDINGS ACTION CARD(Suggested Strategies)		
Key Threat	Potential Triggers	Risk Width
Loss of specialist staff	Severe Weather, Bomb / Explosion Large scale disaster	All services and staff
Risk Strategies		
<p>1. Actions to be considered in the event of a building disruption or loss</p> <p>Threat Strategies:</p> <p>2. Asset Replacement</p> <p>3. Alternative Location</p> <p>4. Home working</p> <p>5. Reciprocal agreements with other LAs</p> <p>All critical services will consider strategies 1-4 as part of the immediate response with option 5 being considered to cover medium or long term by the Strategic Management Group</p>		
Actions To Maintain Service	Timing	Accountable
Advise operational staff of requirement to remain clear of building affected by phone using staff contact lists / SMS text service / Local radio	< 1 hr	Service Managers / Response Group
Invoke Service Business Continuity Plans	< 1 hr	Service Manager
Convene the Response Group (See BCG Task list)	<1 hr	Response Group
Activate <a href="#">[Email address REDACTED]</a> to provide information to staff. If required	<1 hr	Safety & Resilience/ Intranet Administrators
Appoint Salvage Team to attend location	<1 hr	Response Group
Assess the partial / loss of building in conjunction with the Emergency Services	<1 hr	Facilities / Estates / Surveyors / Salvage Team
Assist Fire & Rescue Service to recover information (paper documents)	<1 hr	Salvage Team
Contact insurer for a loss adjuster	<2 hrs	Insurance Officer / Response Group
Assess ICT network disruption and possible workarounds i.e. setting up alternative workstations, diverting numbers	< 4 hrs	Digital
Identify the minimum service levels for the critical services that apply (i.e. that should be recovered) during the incident. Identify those less critical services that can be scaled down or stopped. Identify how long reduced service standards can be enforced before becoming critical before issues such as service capability is seriously affected or non operational. Identify any statutory implications for relaxed standards or scaled down services. Be aware of irregular but time critical events such as elections.	<4 hrs	Response Group
Devise and activate communications strategy to advise key stakeholders	<4 hrs	Comms

Where possible divert customer facing functions to another available service. Divert key staff to an alternative location.	<24 hrs	Response Group / Assistant Director / Estates
Identify any additional support services required to enable staff to focus on service provision e.g. counselling, food on site, flexible working, childcare etc.	<24 hrs	People and Change / Unions
Assign cost code for business continuity incident	1 - 2 days	Finance
Record all expenditure incurred as a result of the incident	As appropriate	All
<b>2. Asset Replacement</b>		
Identify and assess the asset / resources gaps (numbers / length of time / requirements)	<24 hrs	Response Group / Assistant Director
Arrangement for replacement equipment / assets	< 24 hrs	Response Group / Procurement / Service Managers
Communicate changes to working practice to key stakeholders	<24 hrs	Comms
Monitor situation/effectiveness of actions taken, stand down arrangements when necessary.	As appropriate	Response Group
<b>3. Alternative Accommodation</b>		
Assess the amount of equipment required to enable critical service to continue. This should include; ICT requirements (including printers), telephony, office furniture, stationery	<24 hrs	Service Manager
Identify the accommodation requirement. Identify suitable council locations for alternative working arrangements in the short term. Contact Estates for viable options. If no suitable accommodation is available consider mutual aid.	< 24 hrs	Response Group / Estates / External Partners
Prepare the alternative work location for suitability. First aid, DSE, Fire Risk Assessment, evacuation procedures. SEE ALTERNATIVE WORK AREA TASK LIST	< 48 hrs	Salvage Team
Arrange for transport provision to move assets	< 48hrs	Facilities
<b>4. Home Working</b>		
NOTE - This option is most appropriate for; <ul style="list-style-type: none"> <li>Flu Pandemic or contagious diseases (reduces risk of infection)</li> <li>Severe weather.</li> </ul>		
Identify staff who are already working remotely (e.g. severe weather) using RAG assessment. Identify and contact staff who should work remotely (e.g. flu pandemic). Using RAG assessment.	<24 hrs by 1000 of working day	Assistant Director
Check the sustainability of expected home working levels, i.e. the IT requirements	<24 hrs	Response Group / Digital
Contact relevant staff via e-mail, telephone or text message.	<24 hrs	Service manager
Activate and use <a href="#">[Email address REDACTED]</a> webpage to maintain communications with remote staff if deemed necessary.	<24 hrs	Safety & Resilience /

		Intranet administrators
Monitor situation / stand down remote working when crisis passed	<24 hrs	Assistant Directors
<b>5. Mutual Aid Agreement with Local Authorities</b>		
Identify and assess either the capability gaps (numbers/length of time/ equipment requirements) or the service/work that needs to be maintained/done.	2 - 3 days	Response Group / Assistant Directors
Seek authority from CLT to approach and discuss mutual aid with other local authorities	2 - 3 days	Response Group
Communicate changes of working arrangements to key stakeholders	2 - 3 days	Comms
Set up new temporary number / script to redirect calls or seek information on website	2 - 3 days	Digital / Customer Services
Authorise additional expenditure to fund arrangements	2 - 3 days	Finance

## APPENDIX G3

DENIAL OF FUEL / UTILITIES ACTION CARD (Suggested Strategies)		
Key Threat	Potential Triggers	Risk Width
Reduction in waste collection / essential services. Staff absence	Industrial Action Oversees Political issues Severe Weather	All staff
Risk Strategies		
1. Actions to be considered in the event of denial of fuel / utilities Threat Strategies: 2. Fuel Plan 3. Home working 4. Car share 4. Reduction or suspension of service 5. Redeployment of staff to help points 6. Mutual Aid		
Actions To Maintain Service	Timing	Accountable
Upon notification of fuel emergency (7 days notice required for industrial action. Depot to check current fuel levels and arrange for additional delivery)	<24 hrs	Response Group
Activate Sussex Resilience Forum Fuel Plan and prepare for response	<24 hrs	Response Group
Identify critical services that will require fuel to carry out function	<24 hrs	Response Group
Encourage home working	<24 hrs	Response Group
Consider promoting car share share scheme	<24 hrs	Response Group
Ensure Pool Cars are available for essential use only. Fill up cars	<24 hrs	Response Group
Liaise with Digital to accommodate an increase in remote working	<24 hrs	Response Group
Consider Mutual Aid to allow staff to swap working locations with other local authorities to reduce travelling.	<72 hrs	Response Group
Redeploy staff to satellite locations to provide a point of contact for customers.	<72 hrs	Response Group
Liaise with Crematorium to review existing gas supply and assist in arrangement to reduce operations.	<72 hrs	Response Group / Crematorium
Fill up available generators for emergency use (In Emergency Planning Store)	72 hrs	Safety & Resilience Team
Investigate hiring generators for essential services such as ICT	48 hrs	Response Group
Consider reducing office locations in protracted scenarios	<14 days	Response Group
Devise media strategy to reduce travel / waste collections / alternative methods	<72 hrs	Response Group / Assistant Directors / Comms
UTILITIES    ADDITIONAL CONSIDERATIONS		
Provide bottled water	<24 hrs	Facilities / Response Group

Place on stand by Emergency Assistance Centres to provide community with place of safety (May be requested by Utilities companies as part of their emergency arrangements)	<24 hrs	Safety & Resilience
Review procedures for fire safety and marshals in the event of alarm failure. Invoke marshals for each location / work area	<24 hrs	Response Group
Prevent use of lifts in the event of intermittent power failure	<24 hrs	Facilities
Safely back up ICT applications and close non essential applications	<24 hrs	Digital
Encourage the use of manual working procedures as part of service Business Continuity Plans	<24 hrs	Response Group / Assistant Directors
Check the status of UPS and if necessary hire in generators	<24 hrs	Digital
Liaise with external partners such as Sussex Police reference CCTV servers	<24 hrs	Digital



**APPENDIX H**

**BUSINESS CONTINUITY REPORT FORM**

(FOR USE IN THE EVENT OF AN ICT FAILURE ONLY - IN ALL OTHER CIRCUMSTANCES USE THE ONLINE FORM)

[LINK REDACTED]

<b>Directorate</b>	
<b>Assistant Directorate / Head of Service</b>	
<b>Name</b>	
<b>Contact Tel No</b>	
<b>Date of Incident</b>	
<b>Time of incident</b>	

<b>Incident Details</b>	
Description of the incident	
How has the incident affected service delivery?	

<b>Current Status</b>	
Green - Localised disruption that can be managed by internal service amendments. Amber - Services reduced or temporarily suspended requiring external assistance. Red - Service suspended impacts severe.	
Green	
Amber	
Red	

Send the report to the Safety & Resilience Team or contact a representative of the Response Group.

**APPENDIX I**

**BUSINESS CONTINUITY IMPACT ASSESSMENT (RAG)**

(FOR USE IN THE EVENT OF AN ICT FAILURE ONLY - IN ALL OTHER  
CIRCUMSTANCES USE THE ONLINE FORM)  
[LINK REDACTED]


**CURRENT STATUS**

Green - Localised disruption that can be managed by internal service amendments.  
Amber - Services reduced or temporarily suspended requiring external assistance.  
Red - Service suspended impacts severe.


**CURRENT ISSUES** What are the current problems? What is being done to recover?

**ASSISTANCE** What help do you need? (If any)

Send the report to Safety & Resilience Team [Email address REDACTED] or contact [Tel No REDACTED]