ADUR & WORTHING

COUNCILS

BUSINESS CONTINUITY

Incident Management Plan
(PUBLIC VERSION)

USE THIS DOCUMENT IN THE EVENT OF A BUSINESS CONTINUITY INCIDENT

QUICK ACCESS	

Document Control

Subject	Business Continuity Management
Document	Incident Management Plan
Author	Lloyd Harris - Safety & Resilience Manager, Adur & Worthing Councils lloyd.harris@adur-worthing.gov.uk 07879412971
Primary Reviewers	Adur & Worthing Council Response Group
Version Control	This is a Google Drive document. The most recent version always remains live.
Last Reviewed	10/07/2020
Review Date	10/08/2021

CONTENTS

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

1.3 Authority

Adur District Council & Worthing Borough Council 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, tactical functions are delegated to the Response Group led by the Director for the Economy.

1.4 Vulnerabilities

1.4.1 Introduction

Risks identified by the Business Continuity Process have been treated to reduce the probability or impact. 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 do not provide an out of hours services. 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 / Portland House

The main administrative buildings of the council are Worthing Town Hall and Portland House and if an incident related to both buildings, remote working would be implemented similar to the COVID-19 business continuity arrangements recently experienced. This method of working has greatly reduced the risk posed by a denial of access to a building. Those services that rely on a physical location to perform their roles have provided a summary of their contingency measures in the Business Continuity platform. 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 take over the Shoreham Centre as an office space.

1.5 Plan Maintenance

This plan will be reviewed annually by the Safety & Resilience Team in consultation with the Business Response Group 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 [REDACTED] or if this fails phone [REDACTED]

2.2.1 Reporting An ICT incident Outside Of Office Hours

There is no out of hours service for ICT. 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.

2.3 Reporting all other incidents in Office Hours

Serious incidents must be reported to the Response Group via the Safety & Resilience Team in APPENDIX C.

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

2.3.1 Reporting all other incidents outside of office hours

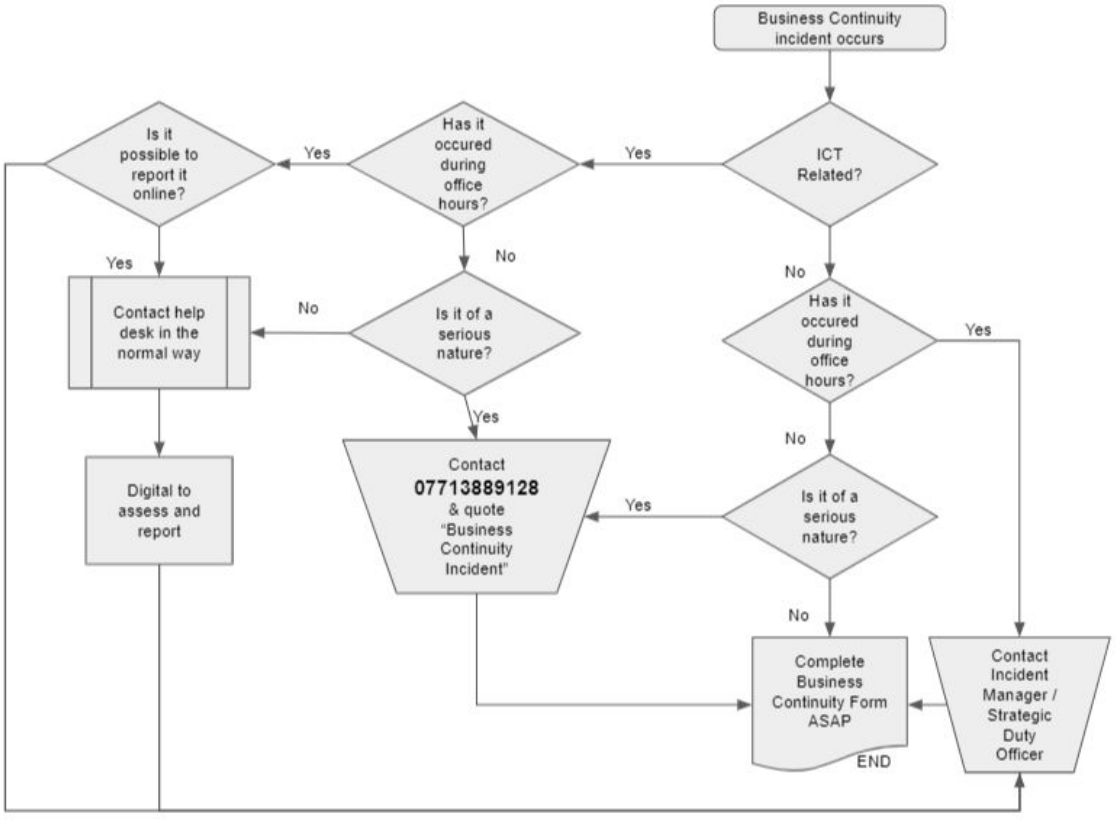
If an incident occurs outside of core working hours the Out of Hours Service must be called immediately quoting “Business Continuity Incident” They will pass the call on to the Incident Manager for assessment and possible activation of this plan and the service business continuity information located on the MATs platform. (APPENDIX C)

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 safety-resilience@adur-worthing.gov.uk for assessment.

The data is compiled on a Google sheet contained within the Business Continuity folder on Google Drive. Once a report has been received, users can click on the responses summary to receive a breakdown of the current situation. A manual copy of the form is stored on Google Drive for printing as required. (See APPENDIX K)

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. Results 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

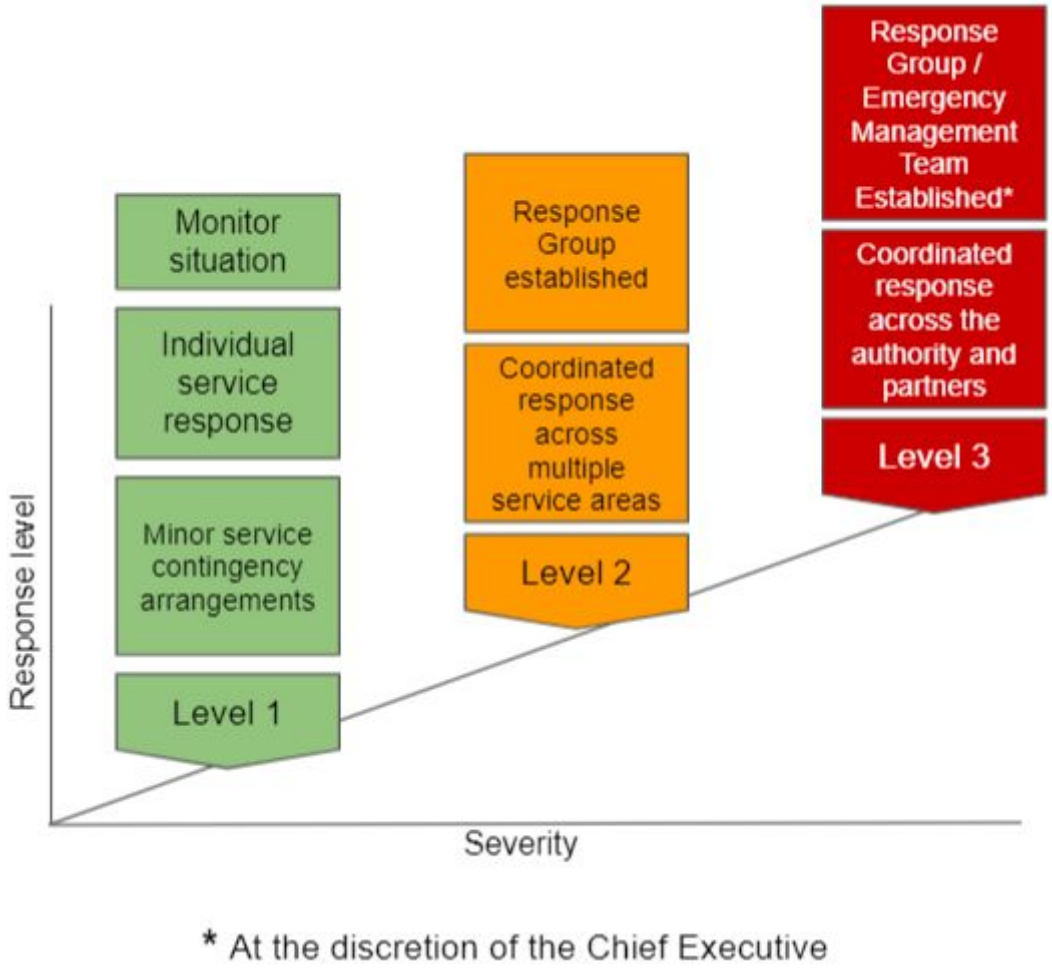
This is defined as an incident causing a significant disruption to the Authority's operations. It may affect an entire building or a number of buildings, employees or visitors, with the escalation potential to require the intervention of the Emergency Services who are likely to take operational control 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 wich affect a local regional or national geographic area.

SECTION 4

4.0 PLAN ACTIVATION

4.1 Plan Activation

The 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 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.

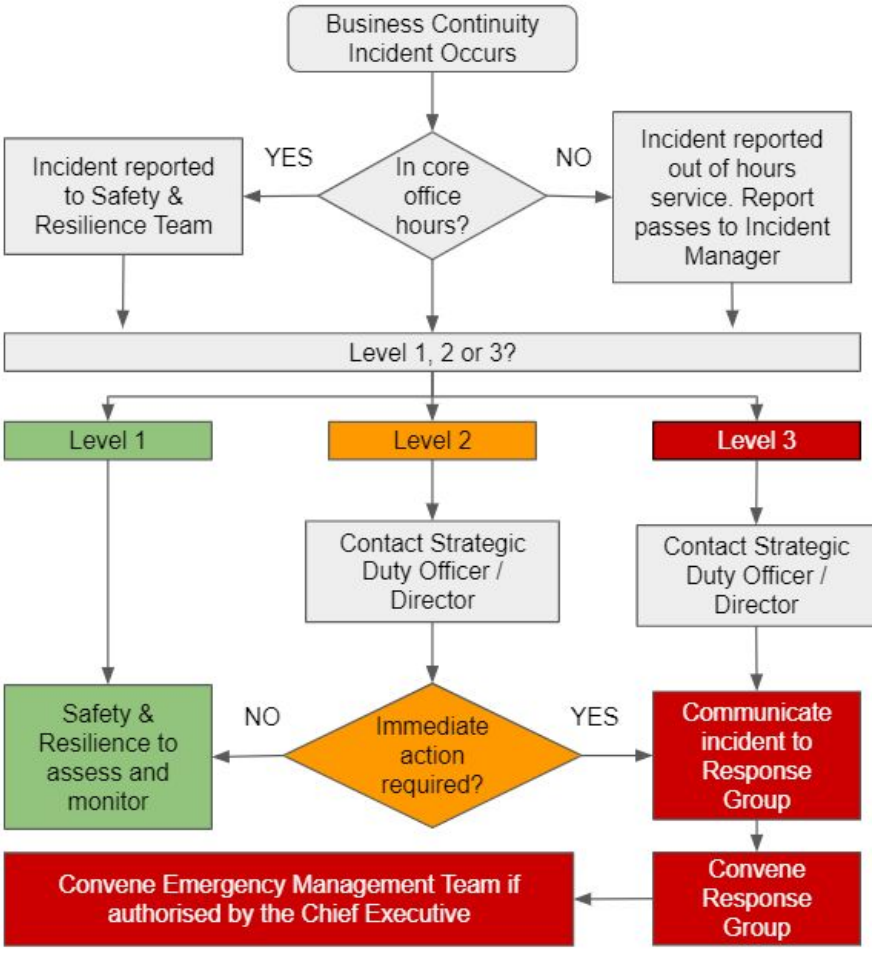
4.3 LEVEL 2 Activation

The Response Group will activate the 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 Council Leadership Team (CLT) in order for an Emergency Management Team to be considered by 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 need for unnecessary travel.
During core office hours the default location for holding Response Group meetings is [REDACTED]. The secondary internal fallback location is Portland House. If there is difficulty in finding an appropriate room within a time critical period, representatives should meet outside the Committee rooms. Precedence must be given over other routine meetings to accommodate this group.

Primary	**Secondary**
[REDACTED]	
Out of Hours Access	
Call the Out of Hours Service on 07713889128 and ask for the “Incident Manager”	

5.1.1 Worthing Fallback Location For Meetings

In the event of both the Town Hall or Portland House become unavailable [REDACTED] have agreed to allow initial meetings to take place.

[REDACTED] **Main line number**	[REDACTED]
[REDACTED]	[REDACTED]
General Email	[REDACTED]

5.1.2 Alternative Locations For Meetings

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

Facility	**Access out of hours**
[REDACTED]	Call the Out of Hours Service on 07713889128 and ask for the “Incident Manager”
[REDACTED]	
[REDACTED]	

5.2 Emergency Control Centre

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.

5.3.2 SMS Text Service

Instructions for transmitting an SMS Text can be found at
See Procedure 1-1 Emergency SMS System

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 or Zoom.
Teleconferencing is also available if technology fails using the “Why Pay” teleconferencing facility
See APPENDIX D

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 [REDACTED]

5.3.5 Emergency Email Address

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

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

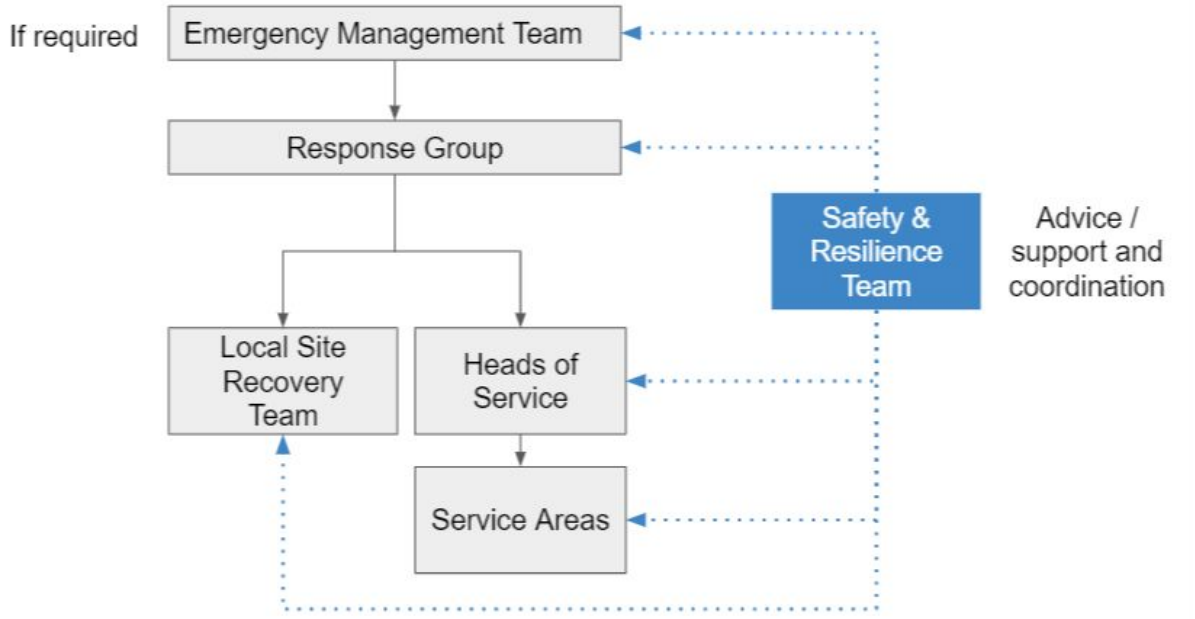
All staff should be encouraged to use this address if and when required.

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.

For information on using the emergency mailbox see APPENDIX E.

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. Heads of Service are ultimately responsible for ensuring impact assessments are completed and submitted within the requested time frame.

The information 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 L.

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 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 resource 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 Emergency Planning Officer)

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 and 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 organisations 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 Operating Picture (COP)

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 J1
Damage / Loss of Building - See APPENDIX J2

Denial of Fuel / Utilities - See APPENDIX J3

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 Head of Communications 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 or Head of Communications.

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 Heads of Service to attend.

6.2 Response Group

See APPENDIX F for meeting agenda and checklist

Standing Members

- Martin Randall - Director for Economy (Chair)
- Steve Spinner - Head of Technical and Business Services
- Jan Jonker- Head of Digital and Customer Services
- Steve Spinner - Head of Business & Technical Services
- Lloyd Harris - Safety & Resilience Manager
- Mark Whitfield - Safety & Resilience Officer
- Paul Tonking - Head of Revenues and Benefits
- Heidi Christmas - Head of Human Resources
- Paul Brewer - Director for Digital and Resources
- Mike Gilson - Head of Communications

LEVEL 1

- 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.

LEVEL 2

- 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.

LEVEL 3

- Report to the Emergency Management Team (if established)

6.3 Emergency Management Team (Strategic)

See APPENDIX J for meeting agenda and checklist

Purpose

The emergency management team will seldom be used as the majority of the functions will be undertaken by the Response group at a tactical level. On occasion however there may be a need to have a strategic only overview of the situation. The Chief Executive will determine whether this extra layer will be required.

Standing Members

All members of the Council Leadership Team. The Group will normally consist of the Chief Executive, or if he was not available, a nominated Director. The team membership will remain flexible depending on the time of incident and the specialist knowledge required to make key decisions. The Chief Executive (or delegated director) has the ultimate authority to request the attendance of any other staff. This group may also include Leaders of the affected councils, Opposition Leaders and nominated Cabinet Members. They would report to the full Council and be responsible for reporting to the community in respect of the incident.

LEVEL 3

- Provide strategic direction in the event of a business continuity incident as identified by the Response Group.
- Liaise with Leaders and Cabinet Leads.
- Provide the authority to suspend services as appropriate.
- Provide the authority to redeploy staff and resources as required.
- Authorise expenditure for large scale incidents.

6.4 Heads of Service / Organisational Leadership Group (Organisational Leadership Group)

See APPENDIX H 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 (Response Group and Emergency Management Team (if established) 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 head of service 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.

6.5 Site Recovery Team (Operational)

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

APPENDIX J1

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

Threat Strategies:
1. Work longer hours in initial phase
2. Move staff internally
3. Home working
4. Reciprocal agreements with other LAs
5. Agency staff

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.

Convene the **Response Group** (Immediately if 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	BRG
Assess the actual/potential loss of staff and distribution of losses across directorates using RAG assessment reporting form.	<24 hrs	RG / OLG
Assess the duration of likely staff loss. Manage absence reporting (for flu) and maintain a log of team staff levels.	<24 hrs	RG / OLG / service managers
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 staff or service user welfare occur. Identify any statutory implications for relaxed standards or scaled down services. Be aware of irregular but time critical events such as elections.	<24 hrs	RG / OLG
Maintain a log of where staff are located to and who has changed their work pattern	<24 hrs	RG / OLG / Service managers
Identify the skill gap – i.e. the shortfall between the staff (and their skills) available and those required to maintain critical services Review the alternatives for closing that gap, see below.	<24 hrs	Service managers
Devise and activate communications strategy to advise key stakeholders	<24 hrs	Head of Comms
Open discussions with trade union representatives on temporary changes to T&C and any enabling support that is required.	<24 hrs	HR / 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	HR / Unions

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	OLG
Consider shorter or alternative work times for staff that have home responsibilities (i.e. schools closed).	<24 hrs	OLG
Make sure H&S is maintained i.e. heating is on, security of building is maintained.	As appropriate	RG / 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 [REDACTED](See Communications)	<24 hrs	RG / Emergency Safety & Resilience / Digital
Brief all other staff on changes to working arrangements	<24 hrs	Head of Comms
Monitor situation/effectiveness of actions taken, stand down arrangements when necessary.	As appropriate	RG / OLG
Identify and assess the staff gaps (numbers / length of time /skills / requirements) - Use RAG assessment form	<24 hrs	RG / OLG
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	RG / HR / OLG
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	RG
NOTE - This option is most appropriate for; ● Flu Pandemic or contagious diseases (reduces risk of infection) ● Severe weather.		
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	OLG
Check the sustainability of expected home working levels, i.e. the IT requirements	<24 hrs	RG / Digital
Contact relevant staff via e-mail, telephone or text message.	<24 hrs	OLG / Service manager
Activate and use [REDACTED] 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	OLG

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	OLG / RG
Seek authority from CLT to approach and discuss mutual aid with other local authorities	2 - 3 days	RG
Consider redirection of calls to another provider.	2 - 3 days	ICT / Customer Services
Set up new temporary number / script to redirect calls or seek information on website	2 - 3 days	ICT / Customer Services
Authorise additional expenditure to fund arrangements	2 - 3 days	Finance

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	OLG
Identify and contact the relevant agency for the staff/skills required.	2 - 3 days	OLG
Notify insurance company when agency staff are employed.		Insurance Officer
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	OLG
Monitor effectiveness of actions, stand down deployment when crisis passed.	As appropriate	OLG

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	RG / OLG
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	RG / OLG
Seek guidance from insurance company	2 - 3 days	Insurance Officer

APPENDIX J2

Key Threat	Potential Triggers	Risk Width
Loss of specialist staff	Severe Weather, Bomb / Explosion Large scale disaster	All services and staff

1. Actions to be considered in the event of a building disruption or loss
Threat Strategies:
2. Asset Replacement
3. Alternative Location
4. Home working
5. Reciprocal agreements with other LAs
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

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 /OLG
Invoke Service Business Continuity Plans	< 1 hr	OLG
Convene the Response Group (See BCG Task list)	<1 hr	RG
Activate [REDACTED] to provide information to staff.	<1 hr	RG / Safety & Resilience/ Intranet Administrators
Appoint Salvage Team to attend location	<1 hr	OLG / RG
Assess the partial / loss of building in conjunction with the Emergency Services	<1 hr	BCG / Salvage Team
Assist Fire & Rescue Service to recover information (paper documents)	<1 hr	Salvage Team
Consider escalation to Strategic Management Group	<1 hr	RG
Contact insurer for a loss adjuster	<2 hrs	Insurance Officer / RG
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	RG
Devise and activate communications strategy to advise key stakeholders	<4 hrs	Head of Comms
Where possible divert customer facing functions to another available service. Divert key staff to alternative location.	<24 hrs	RG / OLG / 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	HR / 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
Identify and assess the asset / resources gaps (numbers / length of time /requirements)	<24 hrs	RG / OLG
Arrangement for replacement equipment / assets	< 24 hrs	RG / Procurement / Service Managers
Communicate changes to working practice to key stakeholders	<24 hrs	Head of Comms
Monitor situation/effectiveness of actions taken, stand down arrangements when necessary.	As appropriate	RG
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	OLG / 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	RG / 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

NOTE - This option is most appropriate for;

- Flu Pandemic or contagious diseases (reduces risk of infection)
- Severe weather.

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	OLG
Check the sustainability of expected home working levels, i.e. the IT requirements	<24 hrs	RG / Digital
Contact relevant staff via e-mail, telephone or text message.	<24 hrs	OLG / Service manager
Activate and use [REDACTED] 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	OLG
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	OLG / RG
Seek authority from CLT to approach and discuss mutual aid with other local authorities	2 - 3 days	RG
Communicate changes of working arrangements to key stakeholders	2 - 3 days	Head of Comms
Set up new temporary number / script to redirect calls or seek information on website	2 - 3 days	ICT / Customer Services
Authorise additional expenditure to fund arrangements	2 - 3 days	Finance

APPENDIX J3

Key Threat	Potential Triggers	Risk Width
Reduction in waste collection / essential services. Staff absence	Industrial Action Oversees Political issues Severe Weather	All staff

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

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	OLG
Activate Sussex Resilience Forum Fuel Plan and prepare for response	<24 hrs	RG
Identify critical services that will require fuel to carry out function	<24 hrs	RG
Encourage home working	<24 hrs	RG
Consider promoting car share share scheme	<24 hrs	RG
Ensure Pool Cars are available for essential use only. Fill up cars	<24 hrs	RG
Liaise with Digital to accommodate an increase in remote working	<24 hrs	RG
Consider Mutual Aid to allow staff to swap working locations with other local authorities to reduce travelling.	<72 hrs	EMT
Redeploy staff to satellite locations to provide a point of contact for customers.	<72 hrs	RG / EMT
Liaise with Crematorium to review existing gas supply and assist in arrangement to reduce operations.	<72 hrs	RG / Crematorium
Fill up available generators for emergency use (In Emergency Planning Store)	72 hrs	Emergency Planning
Investigate hiring generators for essential services such as ICT	48 hrs	RG
Consider reducing office locations in protracted scenarios	<14 days	EMT
Devise media strategy to reduce travel / waste collections / alternative methods	<72 hrs	RG / Comms / OLG
Provide bottled water	<24 hrs	Facilities / RG
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	RG
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	ICT
Encourage the use of manual working procedures as part of service Business Continuity Plans	<24 hrs	RG / OLG
Check the status of UPS and if necessary hire in generators	<24 hrs	ICT
Liaise with external partners such as Sussex Police reference CCTV servers	<24 hrs	ICT

APPENDIX K

BUSINESS CONTINUITY REPORT FORM

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

Communities	DATE
Digital & Resources	TIME
Economy	
Customer Services	NAME
Chief Executive	CONTACT NUMBER

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

Send report to [REDACTED] or contact a representative of the Response Group

APPENDIX L

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

[REDACTED]

Communities	DATE
Digital & Resources	TIME
Economy	
Chief Executive	NAME
	CONTACT NUMBER
Service / Business Unit	

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

Send report to Safety & Resilience Team [REDACTED] or contact [REDACTED]