ANNEX 2

LPP
Local Pensions Partnership

Local Pensions Partnership Group (LPP)

Business Continuity Plan (BCP)

NOTE:

If an emergency occurs which threatens life, property or the environment, your first action should always be to contact the emergency services by dialing 999.

Table of Contents

SECTION 1 - ABOUT THE PLAN

1. Introduction

This is the Business Continuity Plan (BCP) documentation for the **Local Pensions Partnership Group,** consisting of the following:

Local Pensions Partnership Investments Ltd (LPPI) the regulated entity,
Local Pensions Partnership Administration Ltd (LPPA) for Pensions Administrations and Risk services.

In the event of a disaster which interferes with the LPP's ability to conduct business from any of its offices, this plan (Business Continuity Plan) will be implemented and followed by Departments, Funcitions, Teams and individuals responsible to coordinate the business recovery of their respective areas and/or departments. The plan is designed to contain, or provide reference to, all of the information that might be needed at the time of a business recovery.

LPP is comprised of a number of companies and office locations. This plan covers all of the offices, although responsibilities may differ depending on the office location.

There is a framework in place to manage the business continuity process, to assist in this there are a set of documents which support the BCP:

- Crisis Communication Plan – providing a procedure to deal with any crisis which may affect LPP.

- ICT (Information & Communications Technology) Disaster Recover Plan –detailed procedures to recover the ICT systems.

- LPPI Team Business Continuity Plans : Individual plans detailing procedures to deal with possible scenarios and on how teams will prioritise
    - Investment Team BC Plan
    - Compliance Team BC Plan
    - Investment Operations Team BC Plan
- LPPA Team business continuity plans

These documents are available on the intranet and copies are held off-site at the Disaster Recovery DR site and on the Business Continuity website.

2. Purpose of the BCP plan

The purpose of this plan and its complementary policies is to ensure that the organisation has a documented and fully functional set of procedures which incorporate both business and ICT services and which is written in sufficient detail to enable the re-instatement of those services within 24-48 hours of a "disaster".

The objective of the Business Continuity Plan is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of a disruption or disaster. This can include short, medium or more long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, extended power interruptions, and other natural or man-made disasters.

The BCP plan will enable the Company to meet its statutory, regulatory, and commercial obligations and initiate "Business As Usual" in the event of a disaster affecting its normal level of service.

Information security is a key consideration in the plan to ensure that the confidentiality, integrity and availability of information is maintained in any eventuality.

3. What is a disaster?

For the purposes of Business Continuity and this manual the term disaster is any situation that the Executive Committee deem to be of a serious enough nature to implement the BC plan and examples are covered in more detail within the crisis communication plan prepared and updated by the Marketing and Communications Manager.

It should be noted that the length of time of the disruption should be taken into account when deciding to invoke the disaster recovery plan. The time involved in bringing services back and the data loss will need to be considered and will be a key decision point.

A disaster is defined as any event that renders a business facility inoperable or unusable, so that it interferes with the organisation's ability to deliver essential business services.

4. Why the need for the plan?.

4.1 LPP Group provides Investment Management (Regulated Business) and Pension Administration services to London Pensions Fund Authority (LPP) and Lancashire County Council (LCC), as well as pensions administration services to a number of local government organisations (see table below) as part of corporate governance requirements and contractual obligations is to ensure that we provide a working business and IT disaster recovery plan within 24 hours of initiation.

4.2 Investment services are carried out by LPP Investments Ltd (LPP I) which is regulated and an FCA registered subsidiary of LPP. Pension Administration Services are carried out by the LPP Administration Ltd (LPP A).

4.3 With a move to greater reliance on the Internet to enable employers, agencies and members to provide information electronically it becomes more and more critical that service can be provided as quickly as possible.

4.4 A key requirement of our contractual agreements is that the business continuity plan is reviewed on a regular basis and that IT Disaster Recovery plans are tested regularly.

5. Scope of the BCP Plan

The BCP Plan is written to allow for:-

The BCP and DRP plans can be implemented within the 24 hour timescale required given that LPP is comprised of a number of companies and office locations.

- As priority, The LPPI must be capable of resuming its BAU functions.
- The Business Continuity Plan is specific in scope to the recovery of core business functions for the continuation from a serious disruptionional incident in any of LPP's facilities to ensure a fully restored operational business perspective at a new site.
- The Business Continuity Plan includes procedures for all phases of recovery as defined in the Business Continuity Strategy of this document. This plan is separate from LPP's Disaster Recovery Plan, which focuses on the recovery of technology facilities and platforms such as critical applications, databases and servers or other required technology infrastructure. Unless otherwise modified, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations.
- The scope of the Business Continuity Plan will ensure staff / employees have the nessesary training, documentation and understanding of what is expected and to ensure a seemless appraoch during execution of the plan.

6. Maintenance and Changes to the Plan

- Maintenance and review of the Business Continuity Plan is the responsibility of the Business Continuity Manager.
- Maintenance and review of the Disaster Recovery Plan is the responsibility of the Head of ICT and Facilities.
- Maintenance and review of the Crisis Comms Plan is the responsibility of the Marketing manager.
- Maintenance and review of the Team Business Continuity Plans is the responsibility of each department head/ Team Manager.
- Maintaining and/or monitoring of offsite office space sufficient for critical functions to meet recovery time frames is the responsibility of the Head of ICT and Facilities.

7. Plan Testing and Procedures

Testing of the Business continuity plan as a functional document is the responsibility of the SMT (Senior Management team) made of select department heads. The test will include scenario testing, desktop walkthrough, simulations and etc. these will be coordinated by the Business continuity Manager

- Team plans, each team manager is responsible for ensuring the workability of their Business Continuity Plan. This should be periodically verified by active or passive testing.
- All plans are to be reviewed annually (November) or if there is a material change warranting an off schedule review.

8. The Business Continuity Team is made up of

- Senior Management
- Senior Managers Team (SMT)
- Business Continuity Manager
- Facilities Manager
- Site representatives (and their deputies)

9. Invocation

To invoke the plan means to **"Activation : Implement BCP"** the plan following a disaster.

9.1 When can we invoke the BC plan

Depending on the location and the type of disaster, the plan may be invoked in isolation of functions, departments, teams, locations or in full.

There will be a designated business continuity site coordinator at each of the sites outside of the main office.

9.2 Business Continuity Coordinators

The business continuity coordinators will be made up of members of staff that have been identified as site representatives and have the responsibility for managing the implementation of the business continuity plan during an emergency or a disruptive event.

These may be the managers at each site or anyone of senior authority (primary contact). They would also have a deputy to ensure reliance isn't on a single resource should the primary contact be unavailable (secondary contact):

Location	Primary contact details	Secondary contact
Preston		
Herts		
Havering		

Their responsibilities include coordinating the steps in the business continuity plan at their respective sites.

10. Who can invoke the BCP plan

- The responsible officer (s), normally the chief executive or the Chief Risk Officer, will authorise the BCP plan to be initiated.
- In the absence of the Chief Executive or the Chief Risk Officer any member of Senior Management Team (SMT) can authorise the initiation.
- In the absence of any Senior Management a member of the BCP team (Appendix A) can seek approval from the Board Chairman and initiate the plan.
- For instance where disaster recovery will be reverted to, there are invocation cards issued to specific members of staff that can invoke DR regarding access to our alternative site in Romford. This list is reviewed annually in line with the access control policy.

11. Activating the plan

The Chief Executive or Chief Risk Officer will delegate to the BCP managers responsibility for the activation of the Business Continuity Plan. At the point the plan is activated the Senior Management Team (SMT) will be informed. All staff members will be contacted and advised of the current situation and what their role will be in the recovery phase.

The Chief Risk Officer is expected to have the personal contact numbers for the members of SMT and the Business Continuity Manager.

Notification of a business interruption may originate from any source. It is envisaged however that it will come from site staff during occupation of premises, or from the landlord security out of hours and possibly one of the emergency services.

The following activation sequence will normally be used when informing personnel of the activation of this plan, staff will be advised of the process via a number of available methods, text messaging service, email comunications, with updates on the site and or phone calls from managers.

There are three phases which follow in the below sequence using **RAG (Red, Amber, Green)** flags as easy identification:

- **Standby : Early Warning phase**
- **Activation : Implement BC Plan phase**
- **Stand Down : Resume Normal Working phase**

"Standby : Early Warning" phase will be used as an early warning of a situation which might at some later stage escalate and thus require implementation of the Plan. A **"Standby : Early Warning"** allows key personnel/officers time to think, brief staff, start an incident log and prepare for the deployment of resources should an **"Activation : Implement BCP"** message be received. This is particularly important if an interruption occurs towards the end of office hours and staff may need to be asked to stay at work until the situation becomes clear. Resources are not normally deployed at this stage (although this will largely depend upon circumstances) and a **"Stand Down : Resume Normal Working"** may follow this type of alert.

The major activities that can take place during this phase includes:

- Emergency Response Measures
- Notification of Management
- Damage Assessment Activities
- Declaration of the Disaster

"Activation : Implement BCP" phase will be used to request the immediate utilisation of staff and resources and activation of the Business Continuity Plan.

In this phase, the Business Continuity Plans are put into effect. This phase continues until the alternate facility is occupied, critical business functions have been re-established, and computer system services restored to LPP's Departments.
The major activities in this phase include:

- Notification and Assembly of the Recovery Teams
- Implementation of Interim Procedures
- Relocation to the Secondary Facility/Backup site
- Re-establishment of Data Ccommunications

"Stand Down : Resume Normal Working" phase will be used to signify the phased withdrawal of any services or functions provided due to activation of the plan with a transition back to the primary facility locations. The stand down order will be given by the manager who will brief staff, stakeholders and customers as appropriate.

12. Business Continuity Organisation Structure

Responsibility for the BCP Plan is managed by three specific levels of management within the company.

Senior Management

As directors and principle officers this group approves the implementation of the BCP plan and for its overall success and accountability.

In the event of any disaster, early warning or downgrade situation the most senior director available will advise the BCP Manager to begin to initiate the phase level process:

- **"Standby : Early Warning"**
- **"Activation : Implement BCP"**
- **"Stand Down : Resume Normal Working"**

Business Continuity Planning Team

This is made up of the members of SMT (Senir Management Team) and the Business Continuity Coorodinators. The Business Continuity Team has the delegated responsibility to **"Activation : Implement BCP"** the plan. The group comprising key managers will oversee the detailed implementation plans, ensure communication with all interested parties is maintained and ensure any emergency purchasing is authorised and controlled.

The names and contact details of the BCP team members can be found in Appendix A.

Team Managers

Once the plan has begun **"Activation : Implement BCP"** phase then the nominated manager from each of the Service Teams will take responsibility for contacting and organising their staff into the appropriate working patterns at the relevant Disaster Recovery Centre.

The team managers will report back to the BCP team with progress, updates and any issues for resolution.

After the initial first 48 hour period when staff are accommodated and we begin to deliver the service, team managers will control their staff teams in the normal manner.

13. About the Disaster Recovery (DR) Centres & the Contract

London/Hertfordshire

LPP has a Disaster Recovery contract with Daisy Group (formerly Phoenix) that in the event of a disaster then staff from either the London office or LPP Herts can be relocated to one of their disaster recovery centres; the primary location being the Romford Office. The contract also cover the provision of a number of servers, desktops, desks and other office equipment.

Fuller details regarding the Daisy Group contract can be found in the Disaster Recovery Plan manual, including a breakdown of the ICT equipment. Provided is a summary of the centres and the contract.

- The LPP contracts with Daisy Group, a specialist provider of business continuity services; the contract covers the provision of computer servers, PC's, printers, Internet access, telephones and fax machines for staff.

- In the event of a disaster where there is free space within the Disaster Recovery centre we may have the option to extend the number of seats above forty but this would be with agreement with Daisy Group and does not form part of our contract.

- The main Disaster Recovery Centre is at Sovereign House, 16-22 Western Road, Romford, RM1 3JT.

- The contract number with Daisy Group for invocation is DR3772; contact with the site can be made at any time but is limitedto authorized staff listed on the invocation list.

- In the event that the Romford site is not available then our alternate sites would be at Uxbridge in Middlesex or Wapping.

- The DR Centre is open for staff on a 24 hour basis and is subject to entry via front desk security.

- The existing contract allows for fourteen weeks of occupation and may extend by the agreement with Daisy and with the payment of additional fees.

Preston

The Preston office is located in Norwest court, Guildhall Street, Preston, PR1 3NU. The services provided for the various government agencies are pension administration and Investment management services. In the event of a disaster there is a co-located data centre in Manchester which can be used to host backup infrastructure and data. In the event of a disaster this data centre would be used until the main data centre in Preston was available again.

- The main Disaster Recovery Centre is at Daisy House, 1 Brindley Road, Manchester, M16 9TR.

In the event of the main office at Preston being unavailable users would be able to log in and work from home where appropriate. However these arrangements will need to be confirmed so we ensure the resources such as connectivity arrangements for all staff is available.

Havering

The Havening office is located in London Borough of Havering, Town Hall, Main Road, Romford, Essex RM1 3BB.

In the event of a disaster (depending on the scenario – unavailability of office) the Havering Business continuity plan will be reverted to.

14. Business Impact Analysis Summary

The purpose of this section is to provide the priority, recovery time objectives and recovery point objectives for each team to be brought on-line at the recovery Centre.

Name of team	RTO	RPO
Investment Operations	24 hours	Previous business day back up or last good backup
Compliance	24 hours	Previous business day back up or last good backup
Risk	24 hours	Previous business day back up or last good backup
Pensions Payroll	24 hours	Previous business day back up or last good backup
Agency contracts	24 hours	Previous business day back up or last good backup
Pension Services	24 hours	Previous business day back up or last good backup
Employer Services	24 hours	Previous business day back up or last good backup
Facilities (scanning)	24 hours	Previous business day back up or last good backup
Investments	24 hours	Previous business day back up or last good backup
Finance	24 hours	Previous business day back up or last good backup
HR & Training	24 hours	Previous business day back up or last good backup
Commercial Business	24 hours	Previous business day back up or last good backup
Corporate Development	24 hours	Previous business day back up or last good backup
Technical	24 hours	Previous business day back up or last good backup
Business Change	24 hours	Previous business day back up or last good backup

15. Accommodation Plan – London

We have more people than we can accommodate at the Disaster Recovery Centre so we will be operating a split two shift system. Note. If the Disaster Recovery Centre has available space then it will be possible to negotiate for additional seats which incur an additional charge to standard contract fees.

The hours of working have been agreed as 8.00hrs to 15.00hrs GMT and 15.00hrs to 22.00hrs GMT although it's possible for the early shift to start before 8.00hrs and the late shift to extend beyond 22.00hrs as required.

Responsibility for ensuring that the correct numbers of seats allocated to each team are filled is the responsibility of each team manager.

The accommodation plan will need to be fluid as some staff can work from home and some for cultural and family reasons may not be able to meet the shift times.

Team	Number	Day	Evening	Remote Access
Senior Executives				
Pension services, including lfepa				
Employer Services				
Client services				
Corporate Development				
Facilities				
Finance				
HR/Training				
ICT				
Investments				
Marketing				
Specialist services				
Business Change				
Investment Operations				
Compliance				
Risk				

16. Accommodation Plan – Hertfordshire

Seats have been provided for LPP Herts staff at the disaster recovery Centre.

The hours of working have been agreed as 8.00hrs to 15.00hrs GMT and 15.00hrs to 22.00hrs GMT although it's possible for the early shift to start before 8.00hrs and the late shift to extend past 22.00hrs as required.

Responsibility for ensuring that the correct numbers of seats allocated to each team are filled is the responsibility of the Herts team manager.

The accommodation plan will need to be fluid as some staff can work from home and some for cultural and family reasons may not be able to meet the shift times.

17. Accommodation Plan – Lancashire

Should the main office for Lancashire be out of commission, the staff would relocate to the DR site .

Where possible staff could work from home and connect to the services remotely.

18. Communication Plan

A number of ways have been identified to keep staff up to date with information about the disaster scenario.

- The Business continuity website (please insert link) website has been created for staff to be able view news/information. Staff are provided with logon/password access.
- Each night we do a data file transfer of HR records including name and address detail to the site.
- We will use the corporate site once restored to broadcast information.
- We will use email to home address where we have details
- We will use SMS where we have phone details.

Staff have been provided with a business card which is re-issued on a periodic basis; this card contains the three contact names and numbers. The card also contains the details of the website address to the BCP site.

19. Scenario assumptions

A number of potential scenarios have been evaluated those which would require a full implementation of the ICT disaster recovery plan and movement of staff to the disaster recovery Centre and a number of partial incidents which could be managed on site. The scenarios are covered in detail within the individual team BCP plans.

SECTION 2 – MANAGING THE BUSINESS CONTINUITY PLAN/PROCESS

1. Process for plan activation

Depending on the site of disaster, the below can be tweaked to suit location. Other than London, The Site Coordinators will be responsible for ensuring that the process below is followed;

As soon as an incident/disaster is reported the BCP process will commence and we move into "standby mode". The following actions will then be undertaken:-

2. Incident/disaster assessment and action plan

If an incident occurs during normal working hours we may not be able to hold any risk assessments as it may be necessary to undertake an immediate evacuation of the office and the following procedure must be followed.

	ACTION	FUTHER INFO/DETAILS	Applicable to all sites?
1	**Evacuate** the building if necessary	Evacuate the building in accordance with your building's emergency evacuation procedures. Use the nearest stairwells. Do not use elevators.	Yes
2	Ensure all staff report to the Assembly Point.	Staff should gather at the designated **Assembly point.** The designated fire officers are responsible for completing this action.	Yes
3	Call emergency services (as appropriate)	**TEL: 999** The fire officers or representatives from the Landlord is responsible for completing this action	Yes
4	Check that all staff, contractors and any visitors has been evacuated from the building and are present. Consider safety of all staff, contactors and visitors as a priority	**Fire officers to manage the process.** Quickly assess whether any personnel in your surrounding area are injured and need medical attention. If you are able to assist them without causing further injury to them or without putting yourself in further danger, then provide what assistance you can and also call for help. **Roll Call**: department managers are responsible for their team's roll call. This is important to ensure that all employees are accounted for.	Yes
5	Ensure log of incident is started and maintained throughout the incident phase	Use a decision and action log to do this. The log template can be found in the appendix of this manual and all Business continuity coordinators must have an electronic template of this form saved on their mobile devices	Yes
6	Record names and details of any staff,	The designated fire officer and HR department are responsible for completing this action	

	contractors or visitors who may have been injured or distressed in the incident.		
7	Forward details of any fatalities or injuries in the incident to HR (depending on scale of incident) and agree action that will be taken.	The HR contact to forward this information to is the HR Manager	Yes
8	Assess impact of the incident to agree response / next steps	The BCP Manager and SMT are responsible for completing this action	Yes
9	Log details of all items lost by staff, visitors etc. as a result of the incident	Facilities officer is responsible for documenting this information	Yes
10	Consider whether the involvement of other teams, services or organizations are required to support the management of the incident	Depending on the incident the following may be approached to assist with incident management: • Personnel • Health and Safety • Legal • Occupational Health	Yes
11	Advise Managers to contact their staff with next steps	Reliance on Team BC plans at this point. All managers must have the contact details for their staff. Depending upon the time of the disaster, people are instructed what to do (i.e. stay at home and wait to be notified again, etc).	Yes
12	Communication	Ensure that staff are updated as often as possible, ensure all staff have business continuity cards and log on details.	Yes

3. Management/BCP meeting

If possible, it will be necessary to for management and the BCP team to meet to determine the cause, effects and plans. If this meeting cannot be held in suitable location then a conference call inviting all parties can be arranged.

The business continuity manager is responsible for ensuring that this meeting is managed.

The following actions should be considered. Note that all items may not be relevant.

Following this meeting all the actions decided upon will be divided between **first 24 hours and the next 24 hours**

NO	Description	Action	Date
1.	Arrange meeting of managment and BCP team. This could be a physical meeting or a virtual conference		
2.	Confirm all available all team members are present and have access to the Business Continuity Plan and the crises communication plan. –		
3.	Overall situation report including nature and extent of the emergency. Summarize any immediate actions taken.		
4.	Assess effect / impact of the situation, take into account:		
4.1	Accommodation - What premises have been affected? Anything key stored in those building(s)? Alternative premises? Mutual aid arrangements?		
4.2	Staff Are staff affected? Consider requirements and needs of vulnerable staff. Agree which staff are required immediately or their capacity to be available. Plan what to do with staff not immediately required. Ensure all staff are contactable and verify contact details.		
4.3	Suppliers/Contractors/Key Customers Are key suppliers, contractors, partners, customers affected by the emergency? What alternatives are available?		
4.4	What internal support activities been affected?		
4.5	Legal and contractual obligations.		
4.6	Telephony - Has this been affected? Any impact?		
4.7	Work - What is the current status? What are we able to do? What are the current priorities? What key activities are affected?		
4.8	Resources - What resources do we require immediately? To what do we have access? Alternatives? Mutual aid arrangements to borrow equipment?		
4.9	Information Technology Is IT available? How long might the loss be of IT? What are the plans should there be short and long term IT failure. The outage would need to be in excess of 48 hours to consider the move to the DR Centre worthwhile.		
4.1	Transportation issues Are there any problems with staff/customer/ supplier transportation; E.g. Fuel, weather or change of premises problems?		

4.1	Health / Welfare issues		
4.1	Utility issues – Has the emergency meant that facilities are affected; i.e. water, electricity, etc.? What contingency plans are in place for utilities/facilities failures?		
5.	Decide future actions/priorities		
6.	Communication to employees – Agree message to convey to staff – Agree which staff required immediately or their capacity to be available and what to advise them. – Agree communication method to be used; i.e. cascade tree and/or separate line with answerphone or separate staff line/mobile into which they can call.		
7.	Media/Public information – agree media message, see crisis communication plan		
8.	Any other business.		
9.	Chairperson to: – Summarize key points – Re-affirm priorities/actions – Decide if and when next meeting/tele conference call is required.		
10.	Authorise the implementation of the BCP plan as per agreed scenario or stand down and return to BAU.		

4. The first 24 hours

After the initial BCP meeting and risk assessment is completed and it has been agreed to begin the BCP process:-

	ACTION	FUTHER DETAILS/ACTION
1.	Begin plan implementation	
2.	Where possible if access can still be made to the relevant office, recover vital assets/equipment to enable delivery of critical activities	
3.	Dependent upon the disaster situation we may need to invoke the disaster recovery plan and instigate recovery of systems alongside the BCP plans. ICT will be authorised to begin the ICT disaster recovery plan and DR company may need to be informed	

4.	The Company Secretary or designate to email the Board outlining the situation and to keep them up to date with developments	
5.	Hold Managers' meeting if possible or begin chain of communication with Managers whereby each is notified with the facts.	
6.	Update the BCP website and intranet with information and notify staff whether the office is operating under normal working conditions or not.	
7.	Contact staff via bulk text, emails to company accounts, emails to personal accounts.	
8.	Managers to determine level of staff availability in their team and begin the process of keeping staff updated with the disaster status and begin planning for staff to resume work at their main office or DR location.	
9.	Ensure a contact numbers are available and the address details of the DR site, if necessary, are published on the BCP website	
10.	Agree policy for extraordinary additional leave where necessary.	
11.	Ensure that the crisis communication plan is updated and all interested parties kept up to date.	
12.	At the end of the first day assess next steps:- Can staff return to office or do we continue with the DR implementation and staff planning	

5. The second 24 hours

	ACTION	**FUTHER DETAILS/ACTION**
1.	Communicating with staff. As the scale of the incident becomes clearer and the BCP team formulates its plans it will be the responsibility of the BCP team to provide a clear message to managers and staff and this will be coordinated by the Communications manager. The message will be delivered by:- a. Updates to Business Continuity website b. Text messages c. Phone calls from managers d. Emails to home address	

2.	Resource plans for the first day of resumption to be confirmed by managers to the BCP team.	
3.	The ICT will finish the restoration of key systems by the end of the 48 hour period.	

6. After the first 48 hours

If the outage is confirmed as of a longer term nature then the BCP team will need to move the organisation to as "business as usual" as possible. A number of issues will need to be addressed:-

The BCP and wider HR team will work with Managers to ensure that the shift rotas (where necessary) are managed effectively and do not cause un-necessary hardship for any staff member.

Clients are kept up to date with regular communications to measure how well we are managing against the SLA's (Service Level Agreement).

Management will need to work with the board to determine the longer plans, we will we return to the relevant office or will accommodation plans need to be considered.

If the disaster means that the organisation will be out of its offices for a longer period but will return to the original office then a number of requirements will need to be considered.

- Not all systems are being re-instated in the first 48 hours and we will need to consider how and when these can be bought on-line and the cost of this additional work valued against agents contract commitments.

- The seats provided at the DR Centre are for skeleton staff coverage but we cannot sustain this for any length time as the shift pattern would affect operational efficiency. Consideration would need to be given to purchasing additional seats at the DR Centre which can be obtained subject to room availability.

- In London, if the organisation does not get its first choice Centre at Romford and has to locate to Uxbridge this will add burden of travel and costs for staff and again would reduce operational efficiency.

7. Restoration of systems

The BCP manual does not detail the process of restoring systems each scenario will have different requirements and details of system restore procedures can be found in the DR manual.

In the event of a full invocation at the DR centre the following priority of applications and systems would be required.

Note, The BCP plan does not take into account restoration of desktops or the re-build of the physical servers, these are covered in the ICT DR plan but the applications needed by priority.

London/Hertfordshire

Priority	System
	Bloomberg
1	Email
2	Altair
3	Team Drives
4	Telephony
5	OpenHR
6	Intranet
7	Dimensions
8	BACS
9	CMS
10	FiSH
11	Employer Site

Preston

Priority	System
1	Email
2	Altair/Image
3	Team Drives
4	Telephony
5	Intranet
6	BACS
7	CMS
8	Employer Site

SECTION 3 – RESUMPTION OF NORMAL SERVICE RETURNING TO BUSINESS AS USUAL

As the full extent of the incident is known we can determine and manage the process of returning to business as usual the following actions should be completed.

	ACTION	FUTHER INFO/DETAILS
1.	Agree and plan the actions required to enable recovery and resumption of normal working practises	Agreed actions will be detailed in an action plan and set against timescales with responsibility for completion clearly indicated.
2.	Return all operations and services to their original form	Implementation of agreed plan.
3.	Continue to log all expenditure incurred as a result of the incident	Use a financial expenditure log to do this
4.	Respond to any long terms support needs of staff	Depending on the nature of the incident, the Business Continuity Team may need to consider the use of Counseling Services e.g. internal Occupational Health involvement or appropriate External Agencies
5.	Carry out a 'debrief' of the incident and complete an Incident Report to document opportunities for improvement and any lessons identified	Use an Incident Report Form to do this. This should be reviewed by all members of the Business Continuity Team to ensure key actions resulting from the incident are implemented within designated timescales
6.	Review this Continuity Plan in light of lessons learned from incident and the response to it	Implement recommendations for improvement and update this Plan. Ensure a revised version of the Plan is read by all members of the Business Continuity Team
7.	Review the Crisis Communication Plan and lessons learned	Update the Crisis Communication Plan with lessons learned. Add them to the Concerto log.
8.	Review the ICT disaster recovery plan.	Review the recovery plans and amend to learn lessons.
9.	Publicise that there is now 'business as usual'	A number of tasks will need to be completed and will include:- Update of website Publish new telephone numbers Consider who needs to know that normal working practices have been resumed e.g. customers, suppliers etc.
10.	Thank everyone involved	preferably by personal phone call or email

SECTION 4 - APPENDICES

Appendix A – BCP Job roles

Included is the job roles required to manage the business processes within the BCP process (some of the names listed may not be members of the BCP team), the name of the staff member expected to manage this process is added but noted that they may not be available and a substitute may be required.

a) Responsible Officer

- In normal circumstance the responsible officer will be the chief executive officer. In their absence, the Chief risk officer assumes the role.

- Responsible for the overall success of the Business Continuity Plan and to provide direction and guidance to the BCP Manager and BCP team.

b) Finance

- Responsible for ensuring that the company can meet its financial obligations.

- Responsible for authorising payments for ad-hoc requirements at the DR Centre

c) Board Support

- Responsible for providing updates to the Chairman and other board members of progress with the "incident" and our recovery process.

- Provide updates to Executive Committee members of progress with the "incident" and our recovery process.

d) Compliance Officer

- Responsible to ensure LPP I can meet its obligations.

- Provide updates to the Responsible Officer and Executive Committee.

e) HR Manager & staff payroll

- Responsible to ensure that all staffing issues are dealt with efficiently and effectively and escalated to the responsible officer and BCP Manager as required.

- Work with all team managers to ensure a smooth transition of service to the DR Centre.

- Ensure that all staff needs including counseling are provided.

f) Communications Manager

- The marketing and communications manager is responsible for the development and maintenance of the crisis communication plan.
- Work with responsible officer and Executive Committee to provide a full communication facility keeping staff and stakeholders updated on our progress.

g) Disaster Recovery Manager

- The Disaster Recover Manager will take responsibility for the planned restoration of the ICT systems in line with the published DRP plan.
- The DR Manager will work in conjunction with ICT staff and PHOENIX technical staff to complete restorations in agreed time scales.
- Report progress and problems with the restoration to the BCP manager.

h) Business Continuity Manager

- Delegated authority to implement and manage the BCP plan.
- Manage the BCP team members.
- Provide updates to the Responsible Officer and Executive Committee.

Appendix B– Team plans

Team plans are held on the intranet

Appendix C - Key External Contacts list

The key contact list is held on the intranet , on the business continuity website and at the battle box in Romford.

Change History Record

Document Title: Business Continuity Plan					
Version No	Description of change	Owner	Approval	Date of Approval	Date of Issue
1.0	First version	Head of ICT	LPP Executive Committee		
2.0	Revised Draft	Senior Operational Risk Officer	Chief Risk Officer		

Distribution
All staff via Intranet
BCP website
Battlebox at Daisy offices Romford