Business Continuity policy / plan

Contents

1.0 Overview

1.1 Aim and objective

Overall aim is to ensure that PSOW returns to effective operation as quickly as possible after a major incident. It is the aim that the office would be back to full operation within 15 working days (3 weeks),following a catastrophic incident which denies the organisation the use of its office and facilities

This is a live document that will be most effective if it reflects the current position.

1.2 Definition of 'Incident' for the purpose of this policy;

For the purpose of this Policy, 'Incident' is defined as any situation that for a sustained period of time prevents the majority of staff from utilising PSOW premises or facilities (general office and/or ITC facilities) thereby having a major impact upon the output of the PSOW as an organisation, such as;

- Unable to enter premises, or premises unsafe or unsuitable e.g. due to flood / fire / other damage etc
- Unable to access or use PSOW ITC facilities e.g. due to flood / fire / theft / other damage etc
- Sustained lack of suitable environment e.g. lack of power, heating, running water, toilet facilities.
- Majority of staff unable to attend PSOW premises e.g. Due major transport issues, health reasons such as disease outbreak etc.

Incidents which cause disruption for less than a full working day may be managed without the need for implementation of this policy in full.

2.0 Business as usual Process

2.1 Business Continuity Policy Review Team

This team will consist of the following;

- Chief Operating Officer (COODOI)
- Corporate Services Manager (CSM)
- Financial Accountant (FA)
- Assistant Manager – Corporate Services
- Management Information Officer
- Policy & Communications Manager (PCM)
- Other members of staff may be called upon to participate in any testing.

The Review team are responsible for conducting a test exercise of this policy on an annual basis. The COODOI will decide the scenario(s) to be tested and the test conditions, ranging from basic desktop exercise involving only the Review Team, to high realism testing involving all staff.

In the event of relevant information brought to light between tests, a special interim meeting of the Review Team may be called. This will ensure that any changes are incorporated as promptly as possible. Unless such a process is followed it is likely that in the event of a major incident the documentation available will not be adequate for the purpose. The results of all tests should be presented to Management Team and the Audit & Risk Assurance Committee.

2.2 Continuity plan location

Whilst this Policy can be located on the PSOW Intranet as with all PSOW policies, in case of lack of IT and/or premises access copies of this Policy are to be held offsite at all times [REDACTED].

2.3 Information kept up to date

It is important that in the course of normal day to day duties outside of any incident management, the following information is kept up to date.

- **Staff contact details to be kept by Line Managers:** All staff must inform their Line manager and Corporate Services of any change to their contact telephone number as soon as possible. Line Managers are to keep up to date telephone contact details for staff within their teams [REDACTED]

- **Wages and staff contact details to be kept by [REDACTED]:** [REDACTED]

- **IT Backup tapes:**
    - **Daily** backup tapes are to be created each working day by Corporate Services [REDACTED}.
    - **Weekly** and **Monthly** Backup tapes are to be created weekly / monthly by Corporate Services [REDACTED].
    - [REDACTED].

- **External contact details:** Corporate Services will issue the CSM and Assistant Manager – Corporate Services on a six monthly bases a report from SAGE accounts detailing existing suppliers and their contact details. [REDACTED].

- **Authority to access off site safes**: [REDACTED].

- **Telepay Codes**: [REDACTED].

- **Spare Cheque Book:** [REDACTED].

- **Spare Debit Card:** [REDACTED].

3.0 Recovery Management

3.1 Initial Assessment

If any member of staff is made aware of a potential incident, they must contact the COODOI or CSM immediately (directly or via their Line Manager).

As soon as the COODOI and/or CSM are made aware of an incident they are required to undertake an immediate and initial assessment of the incident and its obvious and immediate implications to the PSOW, and the immediate actions required. This may require a site visit if the incident is out of hours. Dependent upon the seriousness of the incident, it may be appropriate to inform the Ombudsman

immediately. The 'Initial Assessment' form (appendix A) can be used as an aid in this initial assessment.

3.2 Initial Communication

Following this initial assessment the COODOI / CSM are to decide;

- What exactly to communicate to Line Managers
  e.g.' the office will be closed for an unknown period due to…., all line managers to contact everyone in their team to inform. Please contact me back to confirm when done'.
  The CSM is to collate names of staff that have not been contacted and consider what further contact attempts can be made.

- What should be communicated to staff via the Line Managers
  e.g. 'the office will be closed for an unknown period due to…., The Line Manager will contact you later in the day with an update.'

- When to begin the information cascade
  e.g. If the incident occurs out of office hours, it may not be necessary to contact Line Managers and or instruct them to contact their staff immediately.

Information will need to be cascaded initially to the Line Managers (and Ombudsman if not already informed). Line Managers are then responsible for cascading this information to all staff within their teams (including Agency Staff and Investigation Associates).

In the event that the COODOI or CSM are unable to contact a Line Manager, it is not appropriate to leave a request to cascade the information in a message .The COODOI and CSM are responsible for ensuring the relevant members of staff are contacted in this instance.

Messages may be left by Line Managers for their staff but it must include a request to acknowledge back to the line manager. Line Managers must contact the COODOI / CSM after contacting their team to confirm names of staff who may not have had the communication.

If possible, Line Managers are to also inform the CSM of any expected visitors to the office (including IPA's). The CSM will then arrange to contact the visitors prior to the meeting to cancel / postpone.

3.3 The Recovery Team

- **The Recovery Team Managers:** In addition to the Ombudsman taking a strategic overview role, the COODOI will be the lead Recovery Manager with the CSM acting as his deputy.

- **The Recovery Team** will also consist of the Investigation Managers (including Review Manager), Policy & Communications Manager, Financial Accountant, Assistant Manager – Casework Support, Assistant Manager – Corporate

Services, Corporate Services Officers and any other members of staff suitable for the incident as deemed necessary by the Recovery Team Managers.

- **Control Centre:** A control centre will need to be established to initiate and manage a recovery plan. The control centre will be based at a location deemed suitable and available dependent upon the circumstances (this may be PSOW offices if any part is accessible / safe / useable). The Recovery Managers are responsible for agreeing upon this location.

4.0 The Recovery Plan

Appendix B is to be used as a checklist for any recovery plan.

4.1 Secondary Assessment: Following the set up of the Control centre, the Recovery Team are to review the initial assessment of the incident regarding the expected effects, the expectations of what is required to be done to effect full recovery and the estimated timescales.

Protection of information and Assets: If there is a risk of any unauthorised access to premises due to the incident the following should be performed assuming access has been deemed safe (following authorisation from emergency services if relevant);

- ensure the premises is secure – enlist a security company if necessary
- safeguard all data on computers
- remove/secure any equipment remaining on site
- remove/secure any documentation remaining on site

4.2 External Communications

Consideration of what to and how to communicate externally is required to be undertaken by the recovery team.

- **The Public:**
  - **Telecoms** - It is essential that the Ombudsman telecom suppliers are contacted to enable an interim message to be communicated to all callers who try to access the Ombudsman's telephone line numbers. (01656641150, 01656641160, 08456010897, 03001231299, and individual staff direct line numbers)
  - **Website** - A communication needs to be posted to the Ombudsman and Complaint Wales websites relating to the possible interruption to services provided by the Ombudsman and any alternative contact routes if known.
  - **Post** - Collection and delivery, including redirection needs will need to be arranged to minimise any delay, possible missing items or items returned to sender unnecessarily. The Post Office Collection Reference for 1 Ffordd yr Hen Gae is FIR816276.
- **The Media / Relevant Bodies / Sister Organisations** The Policy & Communications Manager is responsible for setting up and overseeing the implementing of an action plan for relevant communication to the Media, Relevant Bodies, Sister Organisations and other relevant persons /

organisations as deemed relevant by the Policy and Communications Team based upon the circumstances.

- **PSOW Main suppliers / service providers.** The Recovery Team can commence contacting the Major Service suppliers to PSOW, to inform them of the incident, temporary contact details and the possibility of stopping services temporarily if applicable and possible. The first contacts that should be made are; IT (CAS & internet suppliers), Communication links (telephone), Postal services, Bank/finance/telepay ,Landlord.

4.3 Premises

As PSOW is a one site office, any disruption to access or suitability of the premises for a sustained period of time would effectively result in the inability of this office to carry out its core function in any significant manner.

The Recovery Plan regarding premises would need to take into account the expected duration of the lack of use of the main PSOW Premises, and also the severity of the lack of access.

Severity; Can any part of the premises be used safely? If so can this be utilised to carry out key functions or possibly more on a temporary basis.

Duration: Is the duration of the lack of premises short term, medium term, or long term / indefinite?

Based upon the answers to the above, a decision would then need to be made as to whether to carry out one or more of the following;

- Close office temporarily with no Core function duties being carried out.
- Skeleton staff only in available PSOW office space.
- Enable staff to work from home via remote access (assuming IT services intact)
- Procure Temporary office space (with appropriate IT and Telecoms)
- Procure Permanent replacement premises and facilities.

If temporary office space is considered appropriate, managed office space will be needed to accommodate the current staff headcount of PSOW. Temporary office space providers can be sourced via the internet.

As well as the managed office space there will be requirement for (if not already included in the office space provision):

- work spaces/desks/chairs adequate for current PSOW staffing requirements (see current floor plans for guidance)
- communication links
- computer points to match staffing requirements
- office management facilities; photocopiers adequate to meet current requirements; postal franking machine; telephones adequate for current PSOW staffing requirements
- car parking facilities for staff
- IT equipment adequate for temporary purpose.

- Initial office stationary equipment and supplies (an emergency supply of relevant PSOW stationary is to be maintained off site by the print supplier).

4.4 Utilities

For outages affecting power / lighting / heating and water, the COODOI and CSM must assess the likely duration of the outage and then make an informed decision as to what actions are to be taken in the immediate short term. It is envisaged that alternative arrangements can be made for unplanned water outages of 1 day or less, and brief outages for power / lighting / heating may be managed locally dependent upon the circumstances and environmental conditions that apply at the time.

For outages exceeding 1 day an action plan must be drawn up detailing what arrangements can be made to minimise / eliminate the effects on PSOW service.

4.5 ICT facilities

All aspects of the computer systems must be co-ordinated through CAS Ltd with current onsite IT support contractor and a Corporate Services Officer in support.

[REDACTED]

In the event of complete hardware failure or loss then the following are in place:

- Detailed specifications for the hardware and a Register of the software are held offsite by CAS Ltd. Specification for replacement servers which can recover the information from the backup tapes is part of the hardware specification.

- An Escrow agreement is in place for all content and content management functions of the Ombudsman's websites managed by Fusion Ltd.

- Escrow agreement is to be in place for the WorkPro content management software.

All other software and hardware is commercially available. Details of the requirements are held by CAS (and Datasharp for telecoms software and hardware, Fusion Ltd for websites content management software).

4.6 Financial

- **HR and Pay information**
  [REDACTED].

- **Banking**
  Bank emergency arrangements:

  - [REDACTED]
  - [REDACTED]

- **Accounting information**

[REDACTED]. The possible delay in accessing this back up data is not deemed sufficient to impact on the Ombudsman's ability to operate.

Essential Financial Information as defined by Financial Accountant is recoverable from the National Assembly website (e.g. annual financial accounts and estimates for current year). This information is available on the website of the Finance Committee of the National Assembly for Wales and on the Paid documents details again held on the same website.

Document Owner	Corporate Services Manager
Policy & EIA approved by management team	22 September 2015
Due date of next Review	Quarter 3 2017/18
For publication to :	Intranet (YES) PSOW website (Yes – Redacted Version)

Appendix A

Business Continuity Initial Assessment Form

Description of incident (including reasons if known)	Start Time & Date of issue	Estimated end time & date of issue (if known)

Services Affected	None / Partial / full	Comment on anticipated duration of service failure
Road /Rail / Public Transport		
Staff resources		
Access to Premises		
Car parking		
Premises		
Power		
Heating / air conditioning		
Lighting		
Door security		
Water		
Toilets		
Internal IT (hardware / Software / network / wifi)		
External IT (i.e. websites)		
Telephones		

Comment on overall impact of above
COODOI / CSM Agreed actions (e.g. full implementation of Business continuity plan)

Business continuity Action Checklist APPENDIX B

Action	Action Owner	Deadline	Completed (Y/N)
Initial Assessment (Appendix A)	COODOI / CSM	Day 1	
Control centre established	COODOI / CSM	Day 1	
Initial Communication to Management Team & Line Managers	COODOI / CSM	Day 1	
Communication to Recovery Team	COODOI / CSM	Day 1	
Confirmation from line managers of Communication to Staff	Line Managers	Day 1	
Secondary assessment • Site visit – damage assessment • Emergency services review • Site security requirement • IT functionality – CAS test • Salvage assessment (IT & Non IT)	CSM	Day 1/2	
External Communications (services) • Landlord • Telecomms action list o Divert all ext to main line o Emergency message on main line • Website o Emergency message • Post • Bank • PSOW main service providers	CSM	Day 1/2	
External Communications (RB/Media) • Media • Relevant Bodies • Sister organisations	PCM	Day 1/2	
Action plan devised for recovery and repair or replacement for affected services / premises.		Day 3/4	
Action plan devised for temporary service until fully recovered (e.g. temporary premises)		Day 3/4	
Action plan devised for staff return to work			
Implement above action plans and communicate to staff at relevant point s (e.g. initially after action plan agreed, then after securing start date of relevant premises and required service infrastructure)			

Business Continuity Testing Form Appendix C

Test scenario	
Test condition (e.g. ranging from desk top exercise by COODOI/CSM only to full realism scenario involving all staff)	
Simulation of … e.g. flood	
Service	Test condition level of availability (i.e. full / partial or none), and until when?
Site Access / Transport	
Staff Availability	
Premises Access	
IT networked services (WorkPro / intranet / emails / drives, IPAD , iphone etc)	
Telecomms services • Office landlines • PSOW mobiles	
Utilities (Electricity/ Water / Heating)	
Other test conditions	

Access to data / information	Comments
Availability / Access to Business Continuity Plan	
Key data access • Access to online banking • Access to Salary / bank details • Access to debit cards • Access to cheque book • Access to payroll telepay codes	
ICT back up data access: • Access to most recent back up tapes (daily onsite / other offsite) • Access to servers • Access to CAS • Access to on site IT advisor	
Control centre agreed & established	
Access to contact details of Recovery team	
Information cascade step 1: Access to contact details of management team	
Information cascade step 2: Line managers access to contact details of their team	
Information cascade step 3: Recovery team access to all staff contact information.	

Comments on completion of Business continuity action checklist (appendix B):

Signed……Date……

Signed……Date……

Signed……Date……

Business Continuity key information location
Appendix D

Key information	Soft copy		Hard copy		Update frequency
	Onsite	Offsite	On site	Off site	

[REDACTED]

Corporate Services Contacts – Priority list					
Category	**Organisation**	**Telephone**	**Email**	**Address**	**Contact Name**
Landlord agents	Peleton				
Other tenant	Macmillan Cancer Research				
Other tenant	Davies Turner Ltd				
Other tenant	Vacant				
Telecoms'	Datasharp				
Postal	Royal Mail				
Website	Kagool (pka Fusion)				
IT support	CAS Ltd				
Onsite IT support	Orbit IT				
Bank	Lloyds Bank – Bridgend Branch				

Intruder alarms	Chubb				
Fire Alarms	Peleton				

Media / Relevant Bodies / Sister organisations contact list **(contact details for relevant bodies or others not listed should be searched for via the internet)**					
Category	**Organisation**	**Telephone**	**Email**	**Address**	**Contact Name**