



MIND IN CROYDON BUSINESS CONTINUITY PLAN

This document describes the main issues that might affect the provision of Mind in Croydon's services and describes courses of action to mitigate any disruption to our services should such events occur.

A more detailed approach to risk management is described in our Risk Management Policy and this Business Continuity Plan should be read taking into account the Risk Management and Health and Safety Policies. All of Mind in Croydon's policies are available on our website at www.mindincroydon.org.uk.

ACCOMMODATION – Fire, flood or other occurrences

Mind in Croydon delivers services from four premises in the London Borough of Croydon. It owns three of these premises and rents one from the London Borough of Croydon.

Should any of these premises become unavailable for use, the manager of that building should contact one of the senior management team to discuss a short, medium and long terms plan to allow the continuing delivery of services. Contact details for key staff, trustees and others are included in appendix 1 of this plan. Depending on the nature of the disruption to service (i.e. a building being seriously damaged by fire will require a different response compared to a temporary inability to use the building because of a gas leak etc) a plan will be put in place. It should be noted that all premises have fireproof safes for the safe storage of chequebooks, memory sticks and other important documents.

In the short term, services can be continued by staff relocating to another of Mind in Croydon's premises or by working from home (if appropriate) using online Office 365 email and cloud based access to data and work mobile phones.

Longer term solutions, including the renting of alternative premises or a longer term delivery of service from other premises will be developed within 48 hours of the disruption to service.

It should be remembered that during the nine months that one of Mind in Croydon's premises was being extended and refurbished a plan was put in place to deliver services and this plan worked well.

INFORMATION TECHNOLOGY

Data backup and disaster recovery details

Mind in Croydon expects all staff to save all data either to a file server or to a NAS (network attached storage) where it will be backed up on a daily basis. Files saved to a desktop or to any other location on their PC will not be backed up.

The arrangement and locations of the servers are as follows (the schematic in appendix shows a diagrammatic view);

PURLEY OFFICE:

1 x Windows 2008 R2 domain server for active directory, group policy and print serving. The operating system and system state are backed up nightly to an on-board hard drive. No user data is stored here.

Purley NAS-A – a significant part of the organisations data is stored here. The NAS is backed up nightly to **Purley NAS-B** with a minimum of 30 days' historical data.

Purley NAS-B – stores backed up data from **Purley NAS-A**. Data transfer is via non-MS Windows protocols using credentials not stored in a Windows registry.

ORCHARD HOUSE:

1 x Windows 2008 R2 domain server for active directory, group policy and print serving. The operating system and system state are backed up nightly to an on-board hard drive. On-line user data is stored here and is backed up nightly to **Orchard House NAS** with a minimum of 30 days' historical data.

Orchard House NAS - stores backed up data from **OH domain server**. Data transfer is via non-MS Windows protocols using credentials not stored in a Windows registry.

FAIRFIELD HOUSE:

1 x Windows 2008 R2 domain server for active directory, group policy and print serving. The operating system and system state are backed up nightly to an on-board hard drive. On-line user data is stored here and is backed up nightly to **Fairfield House NAS** with a minimum of 30 days' historical data.

Fairfield House NAS - stores backed up data from **FH domain server**. Data transfer is via non-MS Windows protocols using credentials not stored in a Windows registry.

COMMON TO ALL LOCATIONS:

Remotely accessed data – a number of users require remote access to data. Remotely accessible data is stored online using a combination of MS Sharepoint sites and Google drive. An instance of each is located on the **OH domain server** and these instances are backed up nightly to the **Orchard House NAS** with a minimum of 30 days' historical data.

Email – this is all cloud based and is provided by MS Office 365.

To summarise the above, all data is backed up nightly along with the system and active directory settings of each server. A complete system image is held for each server and these are updated with each nightly backup.

Should a disaster occur to any or all of the above locations it will be possible to restore all or part of the system to its pre disaster state.

PROVISION FOR DISRUPTION TO SERVICE CAUSED BY EXTREME WEATHER CONDITIONS

Preparation for Extreme Weather

A member of the senior management team will aim to inform staff in advance of severe weather warnings for our area so that staff can prepare for potential difficulties.

If extreme weather, likely to seriously disrupt travel, is predicted then the following steps should be taken in advance:

Line managers should ensure that:

- All staff that they manage have the home contact number/mobile for their line manager
- Contact details have been collated for all clients or professionals who have appointments with staff over the next couple of days
- Discussions have taken place with each staff member that they manage about the potential for working at home (potentially through remote access) if staff are unable to get into work

Staff should ensure that:

They have a discussion with their line manager to cover the issues outlined in above.

Procedure for Responding to Extreme Weather

Extreme weather can have widespread implications for the operation of the agency including potential cancellation of appointments and lack of cover for staff who are able to get into work. Consequently, in these rare circumstances, staff are expected to make themselves available for conversations with their line manager earlier than their normal working hours.

The procedure to be followed on a morning affected by extreme weather is:

Between 8am – 9am all staff who would normally be working on that day must make contact with their line manager to inform them if they are likely to have difficulty getting into work. The line manager is responsible for agreeing whether staff are expected to try and get into work and if this is not deemed practical or safe, then agreeing arrangements for cancelling any appointments and agreeing what work may be undertaken from home.

Line managers will make contact with a member of the senior management team, again between 8am and 9am, to inform them of the outcome of discussions with staff so that any decisions can be made about the overall cover in the agency.

Staff are able to undertake much of their work from home using laptop computers to access online Office 365 email and cloud based data in addition to mobile telephones which have been issued to staff.

This procedure should be repeated for any subsequent day affected by extreme weather.

In the case of the counselling service it is expected that the Counselling Manager, in conjunction with the senior management team, will make the decision about whether volunteer counsellors should or shouldn't be expected to try and get into the agency.

If it is agreed that counselling appointments should be cancelled, then the Counselling Manager will make contact with the relevant counsellors and will check if any of their clients have particular needs that require a personalised response to cancelling their appointment. The Counselling Manager will then take responsibility for cancelling appointments with clients.

It is generally expected that staff will make reasonable efforts to get into the agency whenever it is practical and safe to do so. This includes exploring alternative routes or methods of travel including public transport or walking for those within 2 miles of the office. As a service working directly with vulnerable people, it is important that we seek to keep the service operating whenever possible. However, staff are not expected to take any undue risks in order to get into work.

If staff do manage to get into work, it is at the discretion of the line manager to agree whether it may be appropriate to close the service early in order to ensure that staff are able to safely travel home.

Review of the plan

This plan will be reviewed annually by the Risk Management Committee and Board of Mind in Croydon

Reviewed and Updated by the Board of Mind in Croydon – April 2017



MIND IN CROYDON

Appendix 1

Key contact details:

Position/Service	Named contact	Emergency contact details
Chair	Peter Beckett	020 8668 4772
Vice Chair	Jo Leck	020 8668 2534
Hon Treasurer	Tony Horton	07956 953574
Chief Executive	Richard Pacitti	07703 196073
Business Development & Service Delivery Manager	Emma Turner	07541 006 973
H.R. & Office Manager	Cara Scott	07590 056864
Finance and I.T. Officer (also prime contact for insurance issues)	Mike Owen	07841 066121
IT Support	Richard Swann (S-Guard Ltd)	07841 066117
Telephone Systems	Global 4	0870 458 2910 01403 272 910
Insurance	Giles (David Williams) Public & Employee Liability	0121 200 4938
Insurance	Weald (Herman) Premises & Contents	01959 56 5678

Appendix 2

