5 Coles Lane, Cambridge, UK, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org
www.optimumpatientcare.org

Policy Number: POL 2800
Version Number: 5.0
Effective Date: 20 FEB 2020
Review Date: 20 FEB 2021

BUSINESS CONTINUITY POLICY

V5.0 06 FEB 2020

This is a Controlled Document. This policy is issued by the Company. Failure to comply with this policy may lead to disciplinary and/or legal action where appropriate. Human Resources Department and/or appropriate delegate should ensure the policy is communicated to all staff and contractors where applicable. The master copy of this document is kept on the Company Policies and SOPs Smartsheet and NAS drive. A copy may be made available on the Company website for public transparency. Staff may print this document for training and reference purposes but are responsible for regularly checking for more recent versions of the document.

AUTHORS	
Name:	Francis K. Appiagyei
Position:	Clinical Manager / IG Lead
AUTHORISATION	
Name:	Chris Price
Position:	Commercial and Legal Director / SIRO
Signature:	
Date:	20 February 2020

CONTENT

ABBREVIATIONS

OPC or OPC UK	Optimum Patient Care Limited
OPRI	Observational and Pragmatic Research Institute/International
POL	Policy
SOP	Standard Operating Procedure
HR	Human Resources
GP	General Practice
NHS	National Health Service
IT	Information Technology
CCG	NHS Clinical Commissioning Group
CRN	Clinical Research Network
IG	Information Governance
SIRO	Senior Information Risk Owner
DPA	Data Protection Act 2018
GDPR	EU General Data Protection Regulation 2016

BACKGROUND

Optimum Patient Care Ltd (OPC) or referred to as 'Company', supports GP practices, commissioners, health researchers and the wider NHS to improve healthcare provision to patients and better patient outcomes.

Unforeseen incidents may occur that disrupt business operations and service delivery. It is important that we have procedures and measures in place to deal with such events that can allow business operations and service delivery to continue. This policy is important because it provides guidance to employees and contractors (where applicable) on the Company's business continuity plan to manage in the event of an incident that causes disruption to normal business.

PURPOSE

This policy outlines the framework and procedures to be followed by employees and contractors (where applicable) in the event of an incident which impacts upon normal business operations and delivery of services.

APPLICABILITY

This policy applies to Company staff, and associated persons such as secondees, third party and freelance contractors. Compliance with this policy is a legal and contractual duty for staff and contractors. Failure to comply with this policy may lead to disciplinary and/or legal action.

RESPONSIBILITY

All Employees and Users of OPC Information Systems must:

- Adhere to this policy and guidance provided.
- Support management in implementing procedures for business continuity.
- Partake in business continuity testing exercises.
- Report any data breaches during implementation of business continuity procedures.
- Maintain professional conduct and behaviour during implementation of business continuity procedures.

Line Managers:

- Ensure their staff adhere to this policy.
- Support management in implementing procedures for business continuity.
- Act as central point of contact for their staff during implementation of business continuity procedures.
- Ensure on-going compliance of their staff with business continuity testing.
- Report any data breaches during implementation of business continuity procedures.

IT Department

- Ensure IT and networks have built in procedures and recovery (backups) to enable business continuity.
- Ensure IT and networks are adequately protected to limit data breaches and service disruption during implementation of business continuity procedures.
- Provide secure and adequate communication platforms for business continuity.
- Undertake regular testing (at least annually) of business continuity procedures.

HR Department

- Ensure there is adequate staff training and awareness on business continuity procedures.
- Support the IT Department in conducting business continuity testing.

Senior Management:

- Ensure that the policy and its procedures are built into Company processes and that there is on-going compliance. This responsibility is delegated to the IG lead as part of the senior management group.

Senior Information Risk Owner (SIRO)

- Ensure policies and measures are in place to protect staff and critical business assets and enable recovery of such assets for business continuity.
- Ensure appointments are in place to implement, test and monitor business continuity procedures.

POLICY

INCIDENT MANAGEMENT PLAN

INCIDENT IDENTIFICATION

An incident or set of circumstances which might present a risk to the continuity of business or services can be identified by any member of staff. When an incident is identified, it is important that the person identifying the incident knows what to do. In the initial stages, this will involve making sure that the right people have been informed. Notify your line manager immediately and/or notify any of the following **Company Emergency Contacts**:

RESPONSIBLE MANAGERS	NAME	CONTACT NUMBER
Commercial and Legal Director / SIRO	Chris Price	01223 967 844 | 07769 227725
Clinical Manager / IG Lead	Francis Appiagyei	01223 967 865 | 07912 650896
IT Manager	Oliver Taylor	01223 967 860 | 07758218227
Technical Manager	Tim Rijkaard	01223 967 832 | 07767 155655
HR Advisor	Josie Ferrante	01223 967 874 | 07740 200 866
HR Lead	Carole Andrews	01223 967 810 | 07789 796013

Incidents which would cause risk to business continuity include but are not limited to:

- Denial of access to key information systems and resources e.g. serious cyber attack
- Unavailability of premises caused by fire, flood or other incidents
- Unavailability of database caused by network disruption or theft
- Major electronic attacks or severe disruption to the IT network and systems
- Terrorist attack or threat affecting transport networks or the office locations
- Significant numbers of staff prevented from reaching Company premises or getting home e.g. bad weather or transport issues
- Theft or criminal damage severely compromising the Company's physical assets
- Significant chemical contamination of the working environment
- Disease or epidemic effecting significant number of staff
- Simultaneous resignations or loss of a multiple number of key staff
- Widespread industrial action e.g. strikes
- Significant fraud, sabotage or other malicious acts

The incident then needs to be assessed for its potential impact on business and services. **The Business Impact Analysis (Appendix A)** sets out the guide for this assessment.

Minor Incidents

These are interruptions or disruptions that are sufficiently disruptive to require the implementation of business continuity procedures. They can be addressed by line managers. They are smaller scale events, affecting one or a small number of staff e.g. localised computer access issues, denial of access to a building area, a minor power cut for a short period. In the event of a Category A or B incident (as defined in **Appendix B**), a business continuity incident should be declared, and a business continuity plan invoked by the manager responsibility for the service or function affected. However, sometimes minor incidents can become major incidents.

Major Incidents or Emergencies

These are incidents which may cause serious harm or disruption to staff, premises or service provision e.g. pandemic disease, acts of terrorism or mass casualty situations, major weather disruptions, serious cyber-

attack, severe damage to Company premises or facilities, etc. Plans to manage these incidents are focused on more serious or larger scale events, e.g. a national emergency, widespread media coverage of an incident.

BUSINESS CONTINUITY INCIDENT DECLARATION

Where more than one service is affected, any one of the responsible managers for the Company can decide to declare a business continuity incident and invoke the business continuity plan to mobilise an effective response across the organisation.

BUSINESS CONTINUITY PLAN: ACTIONS FOLLOWING INCIDENT DECLARATION

If the incident is categorised as a major incident, a **Business Continuity Team** must be formed to manage the incident. In summary, the actions are:

- Nominate a **Business Continuity Team Leader** (any senior manager)
- Team to operate from an incident control centre, which will be 5 Coles Lane, Cambridge, CB24 3BA or a suitable alternative location
- Follow the Escalation Flowchart (**Appendix E**)
- Systematically review the situation and maintain overall control of Company response by following the guide in the table below:

Manage the Incident	• Start documenting information and actions. • Establish the nature of the incident and assess its impact on the Company's critical functions. • Take any actions required to ensure Category A Functions continue unhindered and Category B Functions can be resumed within 3-7 days. • Ensure Health and Safety of staff is prioritised. • Ensure measures are in place to protect Personal or Confidential information. • Follow the guidance **Action Cards** provided in Appendix C.
Communicate	• Where a major incident has been declared, escalate according to the Escalation Flowchart (**Appendix E**). • Ensure that staff are briefed about the incident and given clear instructions, including, if applicable, on whether they should relocate or go home, and when they are expected to return. • Contact key stakeholders as necessary, e.g. clients of current projects, collaborators, partner CCGs and health boards.
Update	• Update staff, contractors and other key stakeholders with continuity and recovery plans and estimated recovery timelines. • All efforts must be made to ensure personal data or confidential information is protected and secured.
Coordinate next steps	• Once the main priorities have been dealt with, consider scaling down the Business Continuity Team. • If an incident is going to go on for more than 2 days, consider a rota for staff within the team and regular hand over for the Team Leader role.
Organise debrief	• Ensure debrief meetings are held and documented with lessons learned captured and recorded. You may consider using the template Incident Briefing Log (**Appendix D**) for this purpose.

BUSINESS CONTINUITY PLAN: COMMUNICATIONS STRATEGY

During a period of disruption to business continuity, it is vital that communication is managed effectively with staff, service users and stakeholders. This plan supports an effective communication approach before, during and after any incident. The Team Leader should work with the Business Continuity Team to ensure clear and consistent communications. The main aims are:

- To deliver relevant communication about the incident to relevant parties
- To ensure communications are sent out in timely manner
- To ensure communications do not raise panic or cause undue anxiety

Stakeholders: These are divided into two categories with specific communications mechanisms for each category type.

- Internal Stakeholders – Staff (employees and contractors) both office based and remote staff, and OPC collaborative network.
- External Stakeholders – Include but not limited to service users/GP practices, CCGs/health boards/federations, CRNs, researchers, partner organisations and OPRI.

Communication methods

The method of communicating and updating relevant stakeholders should be discussed as part of the business continuity plan. Please ensure the communication method is appropriate for the relevant stakeholder. The communication must reflect the gravity of the incident. Communication guidance is provided in the table below:

Internal Stakeholders	It is essential that to keep staff and contractors informed during a business continuity incident. The methods of communication for internal stakeholders may include: • **Face to face meetings or Teleconference** – ideal form of communication to staff to allow for group awareness, questions and shared decision making. • **Text message/ Phone** – used to disseminate an initial message about the incident, containing immediate actions needed and how further messages will be communicated. • **Email** – Staff can receive messages via the OPCs distribution lists (held electronically) in normal working hours • **Company Website and Social media** – Staff can get up-to-date information via the Company website and social media without having access to Company specific IT systems. • Any updates on these platforms must be approved by senior management.
External Stakeholder	It is essential that to keep external stakeholders informed during a business continuity incident, the expected time for resolution and the expected impact on service delivery to the relevant stakeholder. The methods of communication for internal stakeholders may include: • **Email** – ideal for officially notifying external stakeholders. This should be an official email signed off by the Company directors and should be sent by a Company director or delegated senior manager. • The notification should include key contact details for the Company during the incident period. • Stakeholders should be advised to visit the Company's website for updates where appropriate.

	• Stakeholders should be advised to disseminate the details of the incident to their staff via their own communication channels. • **Phone** – For specific stakeholders, it may also be necessary to notify via phone call in addition to the notification email. • **Company Website and Social media –** Information may also be made available to service users and stakeholders on the Company website and social media where appropriate. • Any updates on these platforms must be approved by senior management.

INCIDENT RESOLUTION OR CLOSURE

All stakeholders, both internal and external, should be notified immediately once the incident has been resolved and normal business resumed.

Any follow-up actions, learnings and preventative measures against future recurrence (if applicable) must be clearly communicated to relevant stakeholder, for assurance and to maintain confidence in the Company.

DISSEMINATION & TRAINING

Dissemination: This document will be made available to staff and contractors via Smartsheet and NAS drive or on request from the HR Department. This may also be in the form of a global notice sent to staff and contractors notifying them of the release of this document or made available on the Company website.

Training: Training on this document will be provided during induction of staff and contractors or as required by their training needs. Additional and/or regular training will be provided as necessary, based on training requirements to ensure continued awareness and compliance with this document.

MONITORING

Failure to comply with this policy may lead to disciplinary and/or legal action where appropriate. Compliance with this document will be monitored by Company senior management or appropriate delegate. This may include regular and/or ad hoc compliance checks and audits where appropriate or warranted. This document is to be reviewed annually or sooner where necessary.

RELEVANT DOCUMENTS

Information Governance Policy
Data Protection Policy
Privacy Notice
Confidentiality Policy
Information Security Policy
Acceptable IT Use Policy
Document and Records Management Policy
Data Quality Policy
Information Incident Reporting SOP
Audits and Monitoring SOP
Staff Handbook

VERSION HISTORY

VERSION	EFFECTIVE DATE	REASON FOR CHANGE	AUTHORS
V1.0	16 SEP 2016	First final version of new policy	F. Appiagyei
V2.0	20 FEB 2017	Annual review and revisions	F. Appiagyei
V3.0	02 MAR 2018	Annual review and revisions	F. Appiagyei
V4.0	22 MAR 2019	Annual review and revisions	F. Appiagyei
V5.0	20 FEB 2020	Annual review, major revisions, new template	F. Appiagyei

APPENDIX A

BUSINESS IMPACT ANALYSIS

Incident	Like-lihood	Effect on Business	Impact	Risk Score	Controls in Place	Short Term Action	Longer Term Action
IT Network Failure	2	No access to email, database, electronic files, telephones	4	8	Email -cloud based Smartsheet -Cloud based Database – Off site backup Telephones- Cloud managed IP phone set up	Remote working using cloud suites.	Restore resource.
Data Loss	1	Loss of information asset for service delivery	4	4	Backup and restore plan	Restore data from on or offsite backup.	No later action necessary.
Fire	1	Loss of use of some or all of premises	4	4	Email -cloud based Smartsheet -Cloud based Database – Off site backup Telephones- Cloud managed IP phone set up	Staff work at home or hot desk at other sites where they have access. Temporary alternative work base for key staff, to enable point of contact and email/internet	Temporary alternative work base for key staff, to enable point of contact and email/internet access. Internal database resources restored
Flood	1	Loss of use of some or all of premises	4	4	Email -cloud based Smartsheet -Cloud based Database – Off site backup Telephones- Cloud managed IP phone set up	Staff work at home or hot desk at other sites where they have access. Temporary alternative work base for key staff, to enable point of contact and email/internet	Temporary alternative work base for key staff, to enable point of contact and email/internet access
Terrorist Attack	1	Loss of use of premises. Possible loss of staff	4	4	Email -cloud based Smartsheet -Cloud based Database – Off site backup Telephones- Cloud managed IP phone set up	Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected.	Temporary alternative work base for key staff, to enable point of contact and email/internet access. Prioritise work if staff affected
Loss of Power	2	No access to email, electronic files, telephones Loss of use of premises	3	6	Email -cloud based Smartsheet -Cloud based Database – Off site backup Telephones- Cloud managed IP phone set up	Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected.	Temporary alternative work base for key staff, to enable point of contact and email/internet access. Prioritise work if staff affected.
Loss of Water	2	Access to Toilets and beverages Cleaning functions	3	6		Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected	Temporary portable toilets Hand sanitizer Bottled water

Loss of Telephone	2	Limited telephone communication. and impact on email/internet?	3	6		Use of mobile phones. If essential staff work from home. Use Mobile internet to retain database access	Temporary alternative work base for key staff, to enable point of contact and email/internet access.
Simultaneous resignation of a number of key staff	1	Loss of leadership function	4	4	3 month notice period in contracts	N/A	Accelerate normal recruitment processes. Seek secondments to cover gap and provide continuity
Staff illness or epidemic	2	Loss of significant number of staff	4	8		Prioritise work.	Prioritise work. Appoint temporary staff where feasible, including secondments from other organisations.
Technical team unable to deliver appropriate support	2	Loss of support staff or business functions	4	8	Provisions for arranging external suppliers to provide support.	Use directly employed staff and/or agency staff to deliver critical functions.	IT Department to remedy. If it cannot, seek alternative sources of support, senior management to arrange agency support.
Travel disruption preventing staff getting to office	2	Loss of significant number of staff	3	6		Staff work at home or at other premises or organisations	As short term, if necessary (long term impact less likely)
Travel disruption preventing staff getting to home	2	Staff wellbeing affected. Disruption to work due to need to accommodate staff.	3	6		Seek alternative methods to get staff home. If possible, obtain food and blankets to enable staff to stay overnight. Potentially look at alternative accommodation for the night.	As short term, if necessary (long term impact less likely)
Widespread industrial action	1	Loss of significant number of staff	4	4	Staff engagement and HR policies	Prioritise work.	Prioritise work. Appoint temporary staff where feasible, including secondments from other organisations.
Theft or damage to assets	2	Loss of use of e.g. computers, furniture, database	3	6	Information Security policies	Staff work at home. Bring old equipment into use. Back up of database restored	Purchase or hire replacements

RISK SCORING		
No	**Probability Scores**	**Impact Scores**
1	Rare	Negligible
2	Unlikely	Minor
3	Possible	Moderate
4	Likely	Major
5	Almost Certain	Catastrophic

5 Coles Lane, Cambridge, UK, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org
www.optimumpatientcare.org

APPENDIX B

INCIDENT CATEGORY AND PRIORITY

Category	Impact	Recovery Timescale
Category A (Critical Function)	Loss of this service would immediately: • Directly endanger life • Endanger the safety of those individuals for whom OPC has a legal responsibility • Prevent the operation of another service in this category • Seriously affect OPC's finances or accuracy of critical records • Prevent communication of vital information	This service must continue to be provided This group will include Services that usually provide a full service 7 days a week, all year
Category B (High Priority/Medium Priority)	High Priority: Loss of Service would immediately: • Present a risk to Health or Safety • Prevent OPC fulfilling a statutory obligation • Prevent the operation of another service in this category • Would seriously adversely affect OPC's reputation	This service must be resumed within 3 calendar days Services included in this group are mainly those that provide a reduced service at weekends and during holiday periods
	Medium Priority: Loss of service would lead to: • Serious knock on effects for the operation of a Critical or High Priority service • OPC's reputation being adversely affected	This service must be resumed within 7 calendar days Services included in this group will include those that normally close during weekends and during holiday periods
Category C (Low Priority)	Loss of this service would lead to: • Potential knock on effect in disrupting the activities of other services within OPC, but no immediate impact upon the provision of Critical or High Priority services	This service should be resumed as soon as practicable. Includes all other service areas that are required in order for OPC to go about its usual business

APPENDIX C

ACTION CARDS

Loss of use of Company offices

In the event of loss of use of Company offices, staff will either work from home and/or arrangements will be made for some staff to temporarily work from a partner organisation's premises or temporary offices. The following actions are recommended:

- Assess likely length of loss of use of offices
- Ensure all staff safe and premises are secured to protect key information assets
- Contact partner organisation to establish availability of usable office accommodation (desks, computer access, meeting rooms, telephone)
- If necessary, obtain IT support to assess capability to establish email and internet links
- Prioritise critical functions as per "Incident Category and Priority" – Appendix B
- Undertake assessment of staff needs – assess which staff can work from home and those that need to work from an office base
- Ensure IT support is in operation for remote working
- Review and reassess the above arrangements daily, ensuring safety of staff and suitability of plans until the Company returns to its offices

Critical loss of staff

In the event of an incident which causes a critical loss of staff e.g. staff illness, terrorist attack, simultaneous resignation of key staff, the following actions are recommended:

- Assess likely possibility of losing more staff
- Ensure all remaining staff are safe and well
- Undertake assessment of staff needs – assess which staff can work from home and those that need to work from the office
- Prioritise critical functions as per "Incident Category and Priority" – Appendix B
- Ask remaining staff to prioritise workload – urgent work or tasks only
- Assess which staff roles need to be replaced most urgently
- Appoint temporary staff where feasible – including secondments from other organisations including OPC collaborative network and OPRI
- Ensure IT support is in operation for remote working for existing and new staff
- Ensure that the stakeholders of affected projects or services are informed as per communications strategy of the above policy
- Review and reassess the above arrangements daily, ensuring safety of staff and suitability of plans until the Company returns to normal staffing capacity

Critical loss of IT systems

In the event of critical loss of Company IT system, the following actions are recommended:

- Assess likely time period that IT systems shall be down for
- Ensure all staff have possible alternative methods of IT access
- Obtain IT support to be able to use back-up systems
- Prioritise critical functions as per "Incident Category and Priority" – Appendix B
- Undertake assessment of staff needs – assess which staff can work from home and those that need to work from an office base
- Ensure IT support is in operation for remote working

- Review and reassess the above arrangements daily, ensuring safety of staff and suitability of plans, until the issue is resolved

Loss of access to internal day-to-day facilities

In the event of loss of access internal day-to-day facilities e.g. water and toilets, the following actions are recommended:

- Report the incident to whom it may concern for repairs or resolution and assess likely time period that the building will be without the facility
- Obtain back up supplies where appropriate e.g. portable toilets, bottled water, etc
- Prioritise critical functions as per "Incident Category and Priority" – Appendix B
- Undertake assessment of staff needs – assess which staff can work from home and those that need to work from the office
- Consider the arrangements for some staff to temporarily work from a partner organisation's premises
- Review and reassess the above arrangements daily, ensuring safety of staff and suitability of plans, until the issue is resolved