RCN GROUP - BUSINESS CONTINUITY POLICY

Version 1
December 2023

Who does this policy apply to?

This policy applies Group-wide for staff, members and all group stakeholders, paid and unpaid, involved in Group activity.

Purpose and description of the document

This policy sets out information for all Group stakeholders regarding our corporate Business Continuity Management (BCM) arrangements in response to major disruption to the business due to the loss or unavailability of:

- key personnel,
- premises/IT or other key resources

Document name

RCN Group Business Continuity Policy

Author/s

Performance, Risk and Assurance Manager, with input from RCNi, RCNF Foundation, Finance, People & OD, Estates and colleagues across the Group

Cross Reference

- Lone Working Policy (staff only)
- Smart Working Policy (staff only
- Taking Time Off Policy (staff only)
- Group Risk Policy (RCN website)
- RCN Group IT Policy (RCN website)
- RCN Group Data Protection Policy (RCN website)

Status and version

Approved – Version 1

Policy owner

Performance, Risk and Assurance Manager

Date policy approved and by whom

Group Audit Committee – **December 2023**
RCN Executive Team November 2023
RCNi Executive Team November 2023
RCN Foundation Management Team October 2023

Date of implementation

January 2024

Date of next review

January 2027

Department responsible for review

Governance Department

CONTENTS

1.0 INTRODUCTION

1.1 In the event of a significant disruption/emergency that affects normal business activities, due to loss/unavailability of:

- key personnel[1], or
- premises, IT or other key resources

The RCN Group ('the Group') is committed to maintaining its key services to members and customers and ensuring that its infrastructure and core functions/processes can continue for staff to carry out their duties. The actions required to achieve this are collectively referred to as business continuity management (BCM).

1.2 This policy reflects the changes to working arrangements across the Group. Group staff can access our systems remotely, therefore the impact on continuing to deliver our services when a Group office is unavailable has now reduced. However, for completeness, this policy does still outline the process when our premises are unavailable and how it could impact on our staff and stakeholders.

1.3 **Definition**

The Business Continuity Institute Good Practice Guidelines (Global Edition, 2013) defines BCM as:

> *a holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.*

1.4 **Policy purpose**

This policy sets out information for all Group stakeholders regarding our corporate BCM arrangements in response to major disruption to business for the areas listed in 1.1 above.

1.5 Such disruption may be due to flood or other severe weather event, fire, terrorist activity, immediate departure of key personnel[1], or a health emergency such as a viral epidemic/pandemic or other regional/national circumstances. The situation may result in loss/unavailability of key personnel[1], power, IT capability, loss of access to buildings, or staff being unable to travel to their workplace or travel on Group business.

[1] includes Executive and Management Teams across the Group, RCN elected members - Council, Country and Regional Boards, RCN and Foundation Committees, RCNi and RCNF Boards, and all appointed external advisers.

1.6 The wide variety of potential causes of such scenarios means it is unrealistic for this policy to give detailed instructions for every possible instance. Instead, it provides guidance on actions to be taken during a period of significant business disruption to help staff to manage and adapt as appropriate, and members and other stakeholders to understand what services and support will remain available.

1.7 The term 'significant business disruption' means circumstances which require a coordinated corporate-level response, either within a specific Group location or across locations and Group areas. The policy does not cover day-to-day events or disruptions that can be addressed within the normal business procedures of a location or Group area and therefore do not require corporate-level coordination.

1.8 This policy and all associated arrangements map to the International Standard for Business Continuity ISO22301 2019. Regular internal audits and monitoring/review of arrangements will ensure the Group's arrangements remain current and fit for purpose in line with this standard.

1.9 This policy should be read in conjunction with the following Group policies and guidance:

- Lone Working Policy (staff only)
- Smart Working Policy (staff only
- Taking Time Off Policy (staff only)
- Group Risk Policy (RCN website)
- RCN Group IT Policy (RCN website)
- RCN Group Data Protection Policy (RCN website)

1.10 Other resources are available on the Safe Working site on the intranet.

2.0 GROUP KEY PRODUCTS AND SERVICES

2.1 The Group provides the following services, which would all be maintained as far as possible in the event of significant business disruption, with possible exceptions as indicated.

2.1.1 The RCN represents the professional interests of nursing staff working in the public, private and voluntary sectors, through negotiation and bargaining with the NHS and independent health and social care sector organisations across the UK, and lobbying government. RCN staff, stewards and reps provide representation, advice and personal support to members in the workplace, in-situ and online.

2.1.2 The RCN Foundation ('the Foundation') is an independent charity providing grants for hardship and education, and processing donations.

2.1.3. RCNi publishes a range of specialist journals, online learning and professional support resources, podcasting and publishing on

current issues in nursing, and organising the annual RCN Nursing Awards.

2.2 If disruption affected the Group and these business activities were reduced, priority would be given to maintaining members' support, membership administration and hardship grants.

2.3 Disruption to core internal functions such as IT, infrastructure etc are considered in section 9 below.

2.4 **Sites affected**
Business continuity plans will consider as necessary how disruption may affect activities at the Group offices. Details on the offices are available on the Group intranet and the RCN website.

3.0 POSSIBLE DISRUPTIONS

3.1 This policy applies to BCM in response to business disruption (according to the definition given in 1.2 above) that impacts on critical services. See Section 7 – Incident response for more details on the types of disruption.

3.2 The table at Appendix A sets out an analysis of scenarios and possible impact (figures range from 1 = least to 5 = greatest). Impacts of 3-5 will require the highest priority in ensuring continuation of the business activities affected.

3.3 In the event of a cyber-attack, it is likely that access would be closed to all staff for at least 24 hours.

4.0 ROLES AND RESPONSIBILITIES

4.1 In the event of significant disruption to business, the following roles and responsibilities will apply.

4.2 The RCN Executive Team, RCNi Executive Team and Foundation Senior Leadership Team (SLT) will provide strategic direction and commitment to the Group's BCM activities.

4.3 At the RCN, the deputy appointed by the General Secretary and Chief Executive (GS&CE , will deputise for the GS&CE when they are unavailable[1]. At RCNi, the Corporate Business Manager will deputise for the Managing Director. At the Foundation, the Head of Grants and Impact will deputise for the Foundation Director.

4.4 A Group Business Recovery Team (BRT) will provide Group decision-making following a critical incident. Details of the BRT

[1] from April 2025, the appointed deputy to the General Secretary and Chief Executive is the Executive Director of RCN Wales.

membership and process for convening are given in the Business Continuity Instruction available on the Group intranet (*access for Group staff only).*

4.5 The BRT will ensure that robust communication networks are in place to allow their decision-making to take place in situations where the emergency means usual communication methods are compromised or non-existent.

4.6 RCN and RCNi Executive Teams and the RCN Foundation SLT will ensure there are appropriate business continuity plans in place, which are tested in accordance with the annual test schedule.

4.7 Executive Directors across the Group, including the Director of the Foundation and the Managing Director of RCNi, will ensure staff are aware of the business continuity and disaster recovery arrangements.

4.8 All staff are responsible for understanding and complying with the local and corporate Business Continuity Planning (BCP) requirements. In March 2022, an online business continuity management training programme was launched for Group staff and is available on ilearn. All staff are required to complete this online course and undertake a refresher course every two years.

4.9 The Executive Director of Governance is the organisational lead for the policy. The Performance, Risk and Assurance Manager manages upkeep and review of this policy.

5.0 GOVERNANCE AND OWNERSHIP

5.1 **Group audit committee**

The Group Audit Committee has delegated authority for business continuity across the Group. Twice a year (normally April and September), the Committee will receive an update on significant incidents at Group or local level. The Committee also approves the annual test schedule (see Section 12).

5.2 **Group wide management**

The RCN Executive Team, the RCNi Executive Team and the RCN Foundation SLT will be responsible for embedding Group-wide business continuity management.

5.3 The Group Business Recovery Team (BRT) will convene following the announcement of an emergency that has Group-wide implications and cannot be managed through normal processes. Group BRT Team members are listed in the document "RCN Business Continuity Instruction - Convening the Business Recovery Team", alongside information on individual roles and responsibilities. This information is available to BRT members at www.support.rcn.org.uk. The Group BRT documentation is

maintained by the Performance, Risk and Assurance Manager (PRM) and held by the Executive Director of Governance and the PRM.

5.4 If the incident is significant enough at Group level, it will be escalated to the RCN Executive Team, the RCNi Executive Team and the Foundation SLT. The business continuity incident reporting form should be completed. The form and criteria for escalating an incident are available on the business continuity home page on the Group intranet (*access for Group staff only).*

5.5 Each of the locations (intranet, RCN website) will have an individual action plan explicitly stating the level of autonomy that local managers are expected to assume if the emergency scenario means Executive Team and / or SLT guidance is unavailable, and the responsibility for BCP processes, decision-making, and management.

6.0 HEALTH, SAFETY AND EMERGENCY SERVICES

6.1 Guidelines for contacting Emergency Services are published in emergency evacuation plans held at each Group location. At London HQ these plans are owned and maintained by the Estates Team. All other plans are owned and maintained by the Executive/Regional/Department Director resident at that location (for freehold buildings) or the building landlord (for leased buildings).

6.2 The Health and Safety Policy covers the RCN and the Foundation, and is available on the Group website (*access for Group staff only*).

6.3 There is a separate RCNi Health and Safety Policy (available on the RCNi website). They set out details of fire safety and prevention, firefighting, roles and responsibilities (eg fire marshals and emergency officers), emergency evacuation procedures, and incident management processes.

6.4 A designated member of the Group BRT will represent the Group in any multi-agency co-ordination and engagement with emergency services.

7.0 INCIDENT RESPONSE

7.1 The immediate response by local managers will depend upon the type and scale of incident. This policy outlines two areas:

- Loss or unavailability of key personnel
- Loss of premises

7.1.1 Loss or unavailability of key personnel[1] (including suspension or departure)

RCN

An AGM/EGM vote could result in the immediate suspension or resignation of an elected member group. The RCN will apply their locally agreed protocols, which document how they will continue to provide core services during any disruption and for brevity, these are not included in this policy. However, a summary is provided below.

Council

- If Council chooses to stand down with immediate effect, election procedures to replace them, including the commencement date for the new Council, will be put in place, in a reasonable timescale.

- The Council may remain until the new Council's term of office commences. If all of Council step down with immediate effect, RCN business will continue until the new Council are in place, but certain decisions might be delayed.

Country and Regional Boards, and Committees

- If a Country board, regional board, or Committee is suspended, disbanded or steps down, election procedures to replace them will urgently be put in place, as soon as is practicably possible.

- The Board or Committee may remain until the new Board or Committee's term of office commences. If they all choose to step down with immediate effect, Council will assume the responsibility of the Board or Committee until the new Board/Committee's term of office commences.

Executive Team

- In the event of the Executive Team resigning, being stood down or disbanded, the recruitment processes to replace the team will begin as soon as is practicably possible. To maintain continuity, the General Secretary and Chief Executive and/or their appointed deputy (see 4.3) and footnote 1 may remain in post until replacements have been sourced.

- If the General Secretary and Chief Executive is suspended or chooses to stand down with immediate effect, the GS&CE's appointed deputy will be appointed on an interim basis. The Chair of Council, supported by the Group Remuneration Committee, will recruit the new General Secretary and Chief Executive.

RCNi

RCNi will apply their locally agreed protocols, which document how they will continue to provide core services during any disruption and for brevity, these are not included in this policy. However, a summary is provided as follows.

Board

- If the Board is suspended, disbanded, or stands down, a recruitment process to replace the board members will begin as soon as practicably possible. The Board may remain until the new Board's term of office commences. However, if all the Board step down with immediate effect, business will continue until the new Board are in place, but certain decisions might be delayed.

Executive Team

- In the event of the RCNi Executive Team resigning, being stood down or disbanded, the recruitment processes to replace the team will begin as soon as is practicably possible. The Chair of the Board will lead the process with input from the RCN General Secretary and Chief Executive. Protocols/plans may include some members of the Executive Team remaining until the new team is in place. Alternatively, RCN Executive Team members may be appointed on an interim basis.

RCN Foundation

The Foundation will apply their locally agreed protocols, which will document how they will continue to provide core services during any disruption and for brevity, these are not included in this policy. However, a summary is provided below.

Board

- If the Board is suspended, disbanded or stands down, recruitment process to replace the board members will begin as soon as practicably possible. The Board may remain until the new Board's term of office commences. However, if all of the Board step down with immediate effect, Foundation business will continue until the new Board are in place, but certain decisions might be delayed.

Senior Leadership Team

- In the event of the Foundation SLT resigning, being stood down or being disbanded, the recruitment processes to replace the team will begin as soon as is practicably possible. The Chair of the Foundation Board will lead the process, with input from the General Secretary and Chief Executive. The Foundation's protocols/plans may include some members of the management team remaining until the new team is in place.

7.1.2 **Loss of premises, including data centres, IT or other key resources**

Some incidents/events may lead to limited or no access to buildings, eg virus outbreak, lack or loss of transport. Other situations may directly affect the availability of IT networks or access to business information, eg network connectivity, Customer Relationship

Management system (CRM) and email, or directly affect the building itself, eg fire, loss of power.

It is important that managers recognise the impact of an emergency may be significantly worse in other parts of the organisation and should react accordingly, seeking status reports on the wider impacts where necessary. Disaster recovery and business continuity plans may need to be escalated if a local incident escalates beyond the control or experience of the employees at the scene or who initially report the incident. The BRT should be informed of any escalation.

7.2 Escalating response to an incident impacting IT (eg cyber-attack)

The Group's reliance on remote working, more so since 2020, means that staff IT requirements are not always linked to a specific office or geographic location. Consequently, the effects of an incident such as cyber-attack can be felt far beyond the Group sites.

All cyber-security Incidents must be reported to the Service Desk in the usual way of logging an IT incident. The Service Desk will log the cyber incident detail and notify the Associate Director of Group Technology Operations, Security and Data and the Information Governance Manager of the incident.

Once identified, a Cyber Incident Response Team will use the Service Desk to log and track the Cyber Security Incident and, as appropriate, take steps to investigate, escalate, and remediate the incident.

The Associate Director of Group Technology Operations, Security and Data and the Information Governance Manager will determine if law enforcement should be informed. They will continue to consult with the appropriate authorities throughout the incident, keeping the BRT informed. The Associate Director of Group Technology Operations, Security and Data and Information Governance Manager will determine if the cyber insurance support should be contacted to engage further support in managing and responding to a cyber incident.

7.3 Escalating an incident response when IT systems and/or infrastructure are impacted, including CRM

Local managers must report incidents to the Service Desk in the usual way of logging an IT incident. The Associate Director of Group Technology Operations, Security and Data will decide if the incident should continue to be managed locally, or if the situation should be escalated. The Associate Director of Group Technology Operations, Security and Data will contact the Communications team to discuss what information should be communicated within the organisation and how.

7.4 Escalating response to an incident impacting staff (eg epidemic, severe transport disruption)

Disaster Recovery and Business Continuity plans may need to come in to effect if an incident:

- leads to levels of staff sickness absence that reduce the Group's effectiveness, or
- leads to absence of staff providing essential infrastructure support (eg Estates or IT staff).

In all instances, local managers must report incidents to the Service Desk in the usual way of logging an IT incident. The Service Desk will assess the extent of any service disruption and appraise alternative solutions.

If the problems impacting staff cannot be resolved by the Estates and IT teams, the Executive Director of Governance should be informed and can consider escalating the situation to the Group BRT.

7.5 Escalating an incident response when Group premises are impacted

Potential examples include:

- fire or other incident requiring intervention of the emergency services
- flood or other incident requiring intervention of external specialists, or
- health and safety breach (asbestos, chemical spillage, water contamination) that may require the advice of the Health, Safety & Wellbeing Manager or intervention by external specialist.

Once made aware of the situation, the Estates Team will co-ordinate the response, working alongside the Health, Safety & Wellbeing Manager, local management, and appropriate external specialists. The Head of Estates and the Associate Director of Group Technology Operations, Security and Data will consider the appropriate action to take and will decide if the incident should continue to be managed locally, or if the situation should be escalated to the Group BRT.

Irrespective of the outcome of that decision, the Head of Estates and the Associate Director of Group Technology Operations, and Security and Data will contact the Communications team to discuss what information should be communicated within the organisation and how.

7.5.1 During working hours

The Head of Estates and Associate Director of Group Technology Operations, Security and Data (or their deputies) must be contacted and informed of the scope and scale of the situation.

The Associate Director of Group Technology Operations, Security and Data is contacted via the IT Service Desk (as detailed in the IT Disaster Recovery Plan); the Head of Estates is contacted using their RCN landline or mobile telephone number.

7.5.2 **Outside working hours**

The building's contracted key holding service will contact the designated local member of staff responsible for the office. The key-holder will have been advised of the contact, who may be someone with easy nearby access to the building rather than a colleague at Director level. The designated contact will make the initial assessment of the scope and scale of the problem. If it requires escalation, they will then contact the Head of Estates and/or Associate Director of Group Technology Operations, Security and Data.

It is recognised that escalating a problem out-of-hours is more difficult and depending on the immediate circumstances there may be no effective action the Group can take until the next working day. This will be considered in the local site's response plan.

7.6 **Evacuating a building**

Emergency evacuation plans are held at each Group building. Adequate means of escape, travel distances, etc, are audited annually as part of the fire risk assessment. Responsibilities for fire safety are set out in the Fire Safety Policy (*access for Group staff only).* For London HQ, the Emergency Evacuation Plan owned by the RCN Estates Team is followed.

For Country and Regional offices (including Cardiff Gate), building evacuation will follow the local processes – evacuation plans for buildings are owned and managed by the local/country/regional directors. Please contact your local office for more details.

8.0 FORMALLY ANNOUNCING AN EMERGENCY AND CONVENING THE GROUP BUSINESS RECOVERY TEAM

8.1 Responsibility for confirming that an incident warrants 'emergency' status lies with the Executive Director of Governance once the incident response has been escalated to them by the Head of Estates and/or Associate Director of Group Technology Operations, Security and Data. In the absence of the Director of Governance, the Performance, Risk and Assurance Manager will take on this responsibility.

8.2 For more details on the Group BRT and the decision making processes, please read Convening the Group BRT.

9.0 RECOVERY

9.1 Recovery management is predominantly the responsibility of the Information Technology and Estates departments. They are responsible for the restoration of critical Group/local infrastructures in the aftermath of an incident.

9.2 How these departments will restore the organisation's key infrastructures are summarised below; more detailed information and processes are held within each department's own documentation.

9.3 **Incident recovery**

The recovery of Group IT infrastructure is led by the Information Technology team, who are responsible for providing core information and communication technology and data processing across the organisation. The continuity of systems and business processes will be assured by incorporating resilience plus incident recovery and contingency planning.

The Information Technology team has adopted a variety of controls to ensure high availability of Corporate Critical systems using methods such as:

- backup and restore procedures
- offsite storage
- cyber-security controls
- antivirus software and procedures
- environmental controls, and
- physical and logical access controls

As we have migrated more and more systems into Cloud-based systems, as opposed to the traditional on-premises server infrastructure, this has naturally shifted the focus of Business Continuity for these systems.

Whilst we still backup the data in the Cloud-based systems, the move to these systems brings much higher resilience levels than could not be achieved without significant capital expenditure in the on-premises environment. This means that the likelihood of a Business Continuity incident for these Cloud-based systems is greatly reduced. However, it does mean that if an incident should occur due to an issue in the Cloud-based Infrastructure, the impact would be the same but importantly we would be reliant on the Cloud provider to resolve the issue.

In the past we have been able to set Recovery Time Objectives (RTOs) that we could test our processes against. These can no longer be tested, as we have no access to create alternate Cloud resources.

It is unlikely that small applications used locally would be included in the Disaster Recovery plans and would not be a priority for restoration.

9.4 **Incident recovery – cyber-attack**

The Information Technology team maintain a Computer Security Incident Response Plan that governs the Group’s general response, documentation and reporting of network and computer-based IT security incidents, such as theft, intrusion, denial of service, and unauthorised access.

The purpose of the plan is to protect the integrity, availability, and confidentiality of the Group’s confidential and proprietary information, to prevent loss of service and to comply with legal and regulatory requirements.

Alongside this plan, the Group takes out a specialised cyber-security insurance policy, covering Legal Services, IT Services, Data Restoration, Reputational Protection Services, Notification Costs, and Credit Monitoring and ID Monitoring.

In the event of a cyber-attack, it is likely that access would be closed to all staff for at least 24 hours.

9.5 **Disaster recovery – Estates**

The Estates team are responsible for the maintenance of the organisation's mechanical and electrical systems and building security in the sites throughout the UK. Details are available at the Group intranet and RCN website. The actions taken by the Estates team to restore any damaged infrastructure are dictated by two questions that need to be asked once the root cause of the incident has been stabilised:

- What is the condition of the infrastructure once the cause of damage has been contained – eg is the office accessible and safe?
- What infrastructure requirements need to be provided to allow business to continue – eg access to alternative RCN accommodation?

The answers to these questions allow Estates to plan the activity necessary to restore the damaged infrastructure and, where needed, assess resources necessary to provide alternative infrastructure to ensure business continuity.

10.0 BUSINESS CONTINUITY DURING AND FOLLOWING THE INCIDENT

10.1 There are three core elements to the Business Continuity plans across the Group and how they are managed are as follows:

- continuity of core functions, for example, financial security of the Group, ie maintaining the movements of money into and out of the Group
- communication with Group staff members and customers across the Group, and
- the local systems and processes (member-facing and departmental) that allow the organisation to maintain its services.

10.2 Continuity of Core Functions

10.2.1 Financial Security

All the organisation's critical financial systems are electronic, and form part of the incident recovery plan for the Information Technology team. However, the nature of the emergency may mean that financial systems cannot be diverted or restored in the short-term and consequently a work-around structure is required.

The Chief Financial Officer and the Associate Director of Group Technology Operations, Security and Data are both members of the Group BRT. Consequently, any impact on the effective financial running of the organisation can be quickly assessed by them and workarounds put into place. See Appendix B for examples.

Not all Group offices manage their Finance functions using the HQ-based team. If an emergency leads to the unavailability of those local finance roles, cover will be provided by the HQ team for an interim period at an appropriate level, under the guidance of the Chief Financial Officer.

If HQ finance staff are unable to work (eg through sickness), Accord Business Solutions ltd (ABS) will be contacted:

- to assess if they have resources available to assist the RCN workload, and
- to ask them to reconfigure existing non-finance systems to allow finance work to be done by Country Finance Teams at the Northern Ireland, Wales and Scotland offices.

10.2.2 Continued provision of Estates infrastructures

If a building has been damaged or is otherwise unavailable, the Estates Team will manage its repair/closure as part of their Incident Recovery processes.

If an office is unavailable, staff will need to work remotely. Hybrid working is now in place across all parts of the Group and the impact of unavailability of a Group office may not have as significant an impact as pre-2020. However, it is still important to outline what steps need to be taken if a Group building is unavailable. The Estates department will work with local management on these occasions.

10.2.3 Provision of Human Resources support to affected Country offices

The People & OD team support all areas of the RCN and the Foundation. This support will continue within the provisions of the BCM plan. The RCNi HR team will support RCNi colleagues.

10.2.4 Continuity of local functions

Local Action Plans and/or Business Impact Assessments (BIA) have been published by every department. These documents identify the impacts to the business when an incident leads to loss or interruption of a department's ability to function. In the aftermath of an emergency, these documents will be used by local management and the Group BRT to assess local requirements over and above the critical corporate functions being restored.

The Group BRT will use the relevant Business Impact Analysis/ Action Plan document(s) to appraise what services and resources require rebuilding, and the priority and timescales of those rebuilds. This will be negotiated in collaboration with the management team at the affected location. The documents allow the Group BRT to investigate alternative resources and infrastructure to mitigate the effect of any incident on resources and service capability. Action Plans are available to the Group BRT by logging in to the RCNs remote Emergency Information website at www.support.rcn.org.uk.

Upkeep of these documents is the responsibility of Executive Directors/Regional Directors and heads of departments across the Group. Owners will update their documents whenever local working methods or infrastructures dictate it to be appropriate; notwithstanding this, all documents must be reviewed annually by management teams.

When a BCP-related document is updated, the local manager is responsible for notifying the Performance, Risk and Assurance Manager, who will upload copies of Action Plans to the Emergency Information website where they can be accessed by the Executive Team and the Group BRT.

10.2.5 Continuity of RCNi and the Foundation

The RCN Foundation stores its electronic file data on the RCN Information Systems. Following an emergency, they will liaise with the Service Desk to restore data in a timely manner.

10.3 Communications

Experience has taught the organisation the value of clear, concise information paths during and immediately following an incident. All local Action Plans must clearly indicate who has responsibility for notifying and liaising with the Communications department, when contact should be initiated, and how communications should be managed.

10.3.1 Communicating with staff

The local senior manager responsible for the site will take responsibility for communications related to the workforce and their work environment, with advice and support from internal communications, People & Organisational Development and RCNi HR teams, eg communicating decisions to open/close offices, communicating health and safety information, and information regarding office relocations.

Once the Group BRT has declared an emergency, it is essential that staff are kept up to date with progress and any decisions that may affect them and their work.

The Group's external website will give staff real-time information and guidance on how to use RCN computer systems and accessing offices. Responsibility for updating the content of the website, telephone recordings and communicating with staff lies with the Internal Communications Department, and all requests to add content must be passed to them for approval and action.

10.3.2 **Communicating with RCN members and Group stakeholders**

The Group BRT will ensure processes are in place to inform Council, RCNi and Foundation Boards, Committees, Activists, Members and other stakeholders of any Business Continuity/Incident Recovery issues, and how these affect members' normal interactions with the Group such as RCN subscriptions and advisory services.

They will also be informed of any alternative measures being put in place to support their continued working (eg alternative office locations, alternative IT infrastructures).

10.3.3 **Communicating with Government, Department of Health and other authorities/statutory bodies**

In circumstances involving, for example, a pandemic or other significant health-related issues, the RCN Group may be called on to offer timely and accurate clinical information and advice to enable healthcare professionals to treat patients appropriately. In such circumstances, the information and the means of communicating it will be negotiated between the external body, the Communications Department and the relevant RCN Group entity/department/region/country.

10.3.4 **Communicating with broadcast media and the public**

All RCN communications with broadcast media must be managed by the media team of the Communications Department. Local/regional Communications Managers will liaise with the central communications team when such communications are dealt with at this level.

RCNi and RCN Foundation communications will be managed locally.

10.3.5 **Communication with all stakeholders regarding a cyber-attack**

In the event of a cyber-attack on the Group, advice will be sought from our cyber-insurance providers to ascertain the appropriate content of all communications with stakeholders. The Associate Director of Group Technology Operations, Security and Data, will coordinate this and work closely with the media team.

10.3.6 **Financial communications between the RCN and Insurers**

Following an incident, it is the responsibility of the Head of Finance (or their appointed deputy) to contact relevant insurance companies and to notify them of the scope and scale of the incident. The Head of Finance will then act as the single point of contact between the Insurance companies and the Group.

In the event of a cyber security event, the Associate Director of Group Technology Operations, Security and Data, will work with the Head of Finance.

11.0 BUSINESS CONTINUITY REVIEW POST-INCIDENT

11.1 Once an incident has been resolved, and business has stabilised, the Group must take the time to review the background to the emergency, the actions that were taken, and the lessons that have been learned.

11.2 Cyber-security incidents involving data categorised as “high confidentiality” or “sensitive data” will be identified to implement the relevant regulatory compliance procedures, if necessary.

11.3 All BCP documentation (both Group and local) is to be reviewed and signed off by the staff lead annually. The reviews should identify any changes to relevant roles/responsibilities, office sites, processes, or systems. All reviews must include a Business Impact Assessment (BIA), which will identify and assess critical IT requirements associated with the plan.

11.4 Reviews should involve contributions from all departments affected by a plan and should also consider implications for the annual budget and planning calendar. Action plans should then be updated and re-issued as appropriate.

11.5 The Performance, Risk and Assurance Manager is responsible for:

- uploading copies of revised action plans to the external website used by the Executive Team and Group BRT, and
- maintaining a schedule that records the dates of action plan updates or reviews, ensuring version control and compliance with the annual cycle.

12.0 ANNUAL BUSINESS CONTINUITY TEST SCHEDULE

12.1 The business continuity test schedule ensures that every location (country and region offices, departments located at Cardiff Gate and London HQ, and the Foundation and RCNi), will be tested at least once every four years. Where possible, testing will be carried out in multiple departments.

12.2 There will normally be six business continuity tests undertaken within the Group annually. In addition, cyber security and penetration tests will be

undertaken annually. The Executive Team and the Group Audit Committee approves the schedule at its final meeting of the preceding year.

12.3 The findings from the tests will be presented to the Executive Team and the Group Audit Committee for consideration twice a year. Any issues raised will be followed up through action planning and review as necessary.

12.4 The Performance, Risk and Assurance Manager (PRA) has responsibility for the annual test schedule as follows:

- the PRA Manager works with the Health, Safety and Wellbeing Manager and Head of Estates to prepare the annual business continuity testing schedule
- the testing programme is approved by the Executive Team and the Group Audit Committee
- the PRA Manager notifies staff leads of imminent BC tests (exact dates are not given)
- on the date of testing the staff leads are notified and the test exercise is undertaken
- staff leads complete the review report template and return it to the PRA Manager, who prepares a summary of completed tests
- the test summary is presented to the Executive Team and the Group Audit Committee twice a year, including updates on changes being implemented as a result of the test exercises, and
- revisions to policies, procedures and systems and learning are completed where applicable.

APPENDIX A - ANALYSIS OF SCENARIOS AND POSSIBLE IMPACT ON BUSINESS DISRUPTION

Type of disruption	Potential causes	Likelihood 1-5	Impact 1-5
Loss/unavailability of key personnel[1]	Outcome of AGM/EGM Ill health Staff headhunted	2 2 3	5 4 4
Loss of staff	Pandemic Epidemic Industrial action Severe weather	4 3 4 4	5 4 2 3
Loss of access to premises	Flood Fire Gas explosion Security threat Disrupted utilities (see below)	2 2 1 4 3	4 4 4 4 3
Loss of premises	Flood Fire Gas explosion Security threat	2 2 1 1	4 (all)
Loss of IT	Cyber-attack* Power outage Severe weather Flood Fire	4 2 2 2 2	5 4 4 4 4
Loss of utilities	Cyber-attack * Power outage Severe weather Flood Fire Contractual dispute	3 2 2 2 2 2	5 3 3 3 3 3
Loss of other critical supplies/contracts	Contractual dispute Market influence	1 1	2 2
Increased security threat	National threat level changed	3	3

* In the event of a cyber-attack it is likely that access would be closed to all staff for at least 24 hours.

[1] includes Executive and Management Teams across the Group, RCN elected members - Council, Country and Regional Boards, RCN and Foundation Committees, RCNi and RCNF Boards, and all appointed external advisers.

APPENDIX B - TEMPORARY WORKAROUNDS FOR EFFECTIVE FINANCIAL RUNNING

Examples of arrangements that will be put in place to ensure financial systems continue to be effective are as follows.

eBIS finance expenses system

There is a single server that holds Open Accounts and eBIS.

A manual intervention will allow the system to be restored in a few minutes.

Direct Debit system

This is performed by the member admin team. It is used for membership, RCNi subscriptions, and Foundation donations.

Systems are in place to allow BACS processes and tasks to be performed at Cardiff Gate (where this activity normally occurs) or from any other RCN office or remotely, providing the necessary RCN IT networks are in place and the relevant personnel are available.

In the event of CRM system failure, retrieval and restoration of the system should be within 24 hours of the Incident Recovery Plan being invoked.

Payroll system

Tests have confirmed that PBS, the organisation which handles payroll systems for the Group, can, if necessary, access our system and run our payroll file in the event of an incident (this assumes the London or Cardiff network is functional). It may also be possible for PBS to submit BACS at the same time.