Doncaster and Bassetlaw Hospitals NHS
NHS Foundation Trust

Information and Communications Technology (ICT)

BUSINESS CONTINUITY POLICY

(including: Disaster Recovery Plans)

Did you print this document yourself?
The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Name and title of author	Roy Underwood – Information Governance Manager Stephen Parsons - Deputy Director of ICT
Date revised	9th May 2012 and February 2013
Approved by (Committee/Group)	Information Governance Group ICT Risk Management Group
Date of approval	18 March 2013
Date issued	28 March 2013
Next review date	May 2015 **– extended to June 2020**
Target audience:	Trust-wide

ICT Business Continuity Policy

Amendment Form

Version	Date	Brief Summary of Changes	Author
Version 3	February 2013 May 2012	• Updated for grammar and new style format included. • Updated to meet current systems and priorities and for departmental structure.	S Parsons S Parsons
Version 2	June 2008	• Minor amendments to content around Head of Information & ICT Services job roles and references to Disaster Recovery Plans (DRP). • Reformatted to comply with NHSLA and Equality Impact Assessment requirements.	Roy G Underwood
Version 1	July 2006	Implementation	Roy G Underwood

ICT Business Continuity Policy

Contents

ICT Business Continuity Policy

1. AUDIENCE

This document addresses several groups within the Trust with differing levels and types of responsibilities for business continuity, as follows:

- Trust Board of Directors
- ICT Services Business Continuity Team
- Trust ICT Services Support Teams

It should be emphasized that this document is addressed particularly to the members of the BCMT, since they have the responsibility of preparing for, responding to, and recovering from any disaster that impacts on the Trust. Part III of this document describes the composition of the BCMT in detail.

2. INTRODUCTION

This document provides the written record of the Doncaster & Bassetlaw Hospitals NHS Foundation Trust's (***the Trust***) ICT Business Continuity and Disaster Recovery Plans.

Introduction to this Document

Planning for the business continuity (ICT Services) of the Trust is a complex task. Preparation for, responding to, and recovery from a disaster affecting the ICT Service functions of the Trust requires the cooperative efforts of many support organizations in partnership with the functional areas supporting the "business" of the Trust. This document records the Policy that outlines and coordinates these efforts, reflecting the analyses by representatives from relevant departments and by the Trust's Information Governance Manager. For use in the event of a disaster, this document identifies the computer recovery facilities (standby sites) that have been designated as backups if the functional areas are disabled. This document is divided into four parts, as described below.

3. PURPOSE

The Trust increasingly depends on computer-supported information processing and telecommunications. This dependency will continue to grow with the trend toward centralizing information technology within the Trust. The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of the Trust.

The Trust's Risk Assessment Framework is an integral component of the Trust's decision to work towards compliance with the Information Security Standard ISO17799. This process is repeated on a regular basis to ensure that changes to our processing and environment are reflected in recovery planning.

The Trust recognizes that there are usually two distinct levels of support required:

- There is a high probability in a large Acute Trust of theft or malicious damage to ICT Facilities. This probability requires us to make plans for a reliable ICT Incident Reporting mechanism coupled with a rapid replacement system for 'lost' facilities which does not generally involve any facilities other than the ICT itself. Repairs or improvements to Physical Security measures in vulnerable areas are largely the responsibility of the Trust's Estates Department.

- There is a much lower probability of severe damage to data processing, network services and telecommunications capabilities that support the Trust. Nevertheless, because of the potential impact, a Policy for reducing the risk of damage from a disaster, however unlikely, is vital. The Trust's ICT Services Business Continuity Policy is designed to reduce the risk to an acceptable level by ensuring the restoration or continuation of critical Category 1 and essential Category II processes. The Policy identifies the critical ICT functions of the Trust and the resources required to support them. The Policy provides guidelines for ensuring that the necessary personnel and resources are available for both disaster preparation and response and that the proper steps will be carried out to afford the Trust timely restoration of services.

- This Business Continuity Policy specifies the responsibilities of the BCMT, whose mission is to establish Trust level procedures to ensure the continuity of the Trust's business functions. In the event of a disaster affecting any of the functional areas, the BCMT serves as liaison between the functional area(s) affected and other Trust departments. These services include the support provided by ICT, Estates, Fire and Security Services, and public information dissemination handled by the Trust's Communication's Office, among others.

3.1 The Main Threats

The Policy is predicated on the validity of the following threats to ICT Service Provision:

- **Threat 1** – Loss of Power

- **Threat 2** – Serious environmental damage to Computer and /or Telephony Rooms/s (explosion, fire, flood etc)

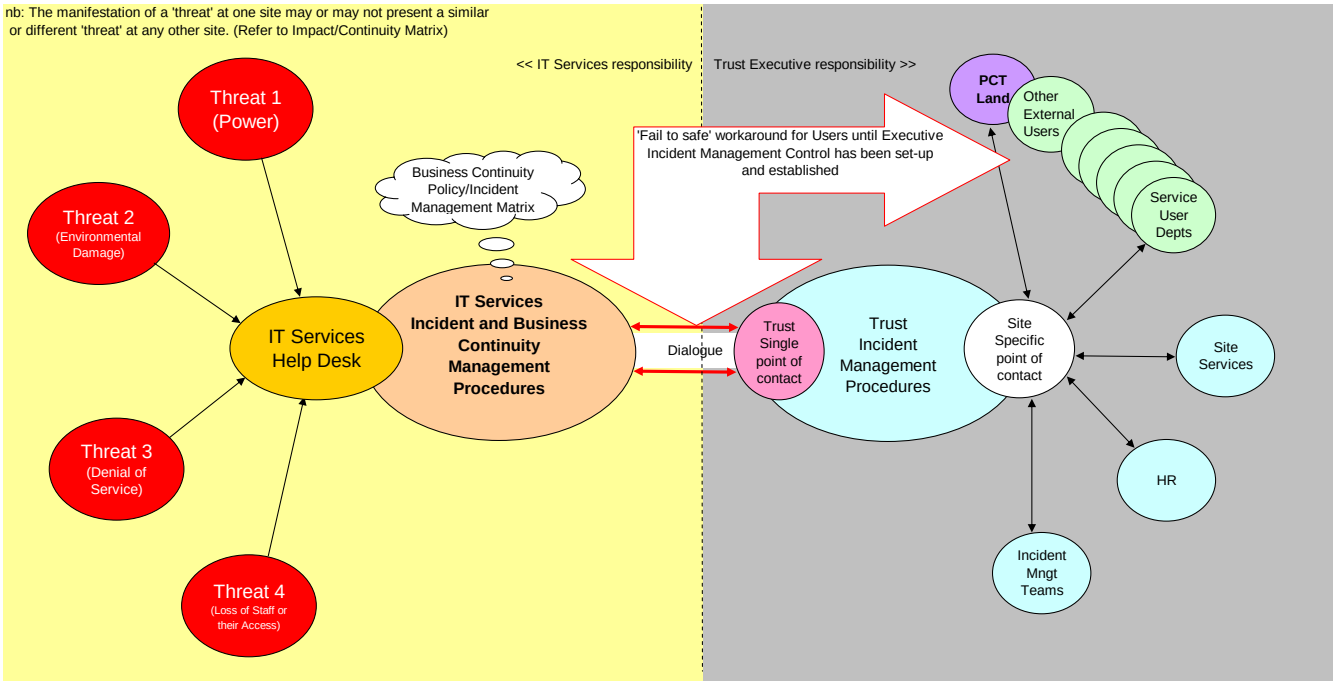
- **Threat 3** – Denial of Service Attack by:
  - Serious software/system malfunction
  - Serious Virus, Trojan Code or Worm

- **Threat 4** – Serious loss of staff (e.g. sickness/strike) or loss of physical access to computer / telephony rooms (e.g. terrorist activity)

Location: Trust-wide: impact would be site specific depending on the Threat manifestation

The Trust's Information Governance Manager, with assistance from the Trust's ICT Support Manager and Internal Audit Services is responsible for developing the Trust's ICT Business Continuity Policy. However, development and support of individual ICT Services Recovery Policies are the responsibility of the functional area planning for recovery. Central to the Policy and indeed the business continuity and recovery processes is the Executive 'single point of contact' between ICT Services and the Users of the services they provide.

3.2 ICT Incident Management Schematic



Ensuring that the Policy reflects ongoing changes to resources is crucial. This task includes updating the Policy and revising this document to reflect updates; testing the updated Policy; and training personnel.

The BCMT are responsible for this comprehensive maintenance task.

Annually, the BCMT Chair (the Deputy Director of ICT), ensures that the Policy undergoes a more formal review to confirm the incorporation of all changes since the previous year, and also initiates a complete review of the Policy, which could result in major revisions to this document.

The Trust Policy Management Team will distribute these revisions to all authorized personnel. Testing the Business Continuity Policy is an essential element of preparedness. Partial tests of individual components and recovery policies of specific ICT Services Teams will be carried out on a regular basis.

A comprehensive exercise of our continuity capabilities and support by our designated recovery facilities will be performed on an annual basis.

4. SCOPE OF THE ICT BUSINESS CONTINUITY POLICY

The object of this Policy is to give guidance on the restoration of Critical and Essential systems in the aftermath of a disaster that disables any functional area and/or essential equipment supporting the systems or functions in that area. The Risk Assessment of the computer applications should assign appropriate Categorization. This Risk based process identifies applications that have the highest priority and must be restored within the timescale of the disaster recovery matrix. Specifically, each function of these systems is evaluated and allocated a place in one of four risk categories, as described below.

Category I - Critical Functions

Category II - Essential Functions

Category III - Necessary Functions

Category IV - Desirable Functions

Note: Category IV functions are important to the Trust administrative processing, but due to their nature and other factors, they can be suspended for the duration of the emergency.

The systems in Categories I - III are those that provide Trust wide services i.e. Patient Systems, Internet and eMail, Medical Records, Office and Ambulance systems[1]. There are many departmental and laboratory systems as well as non-information processing systems that are also either essential for the Trust or the local area(s) they support i.e. Rotherham, Doncaster and South Humber Mental Health NHS Foundation Trust and the Doncaster Primary Care Trust. Recovery for these systems too must be based upon Service level Agreements, an assessment of the impact of their loss and the cost of their recovery.

The helpdesk will decide – based on information available at the time of the incident – on the seriousness of the incident:

- Major - BCP action
- Medium - Helptrac action
- Minor - Helptrac action

Disaster Recovery → Full BCP

Significant Issue → Matrix Only

Run of the mill issues
(May require Matrix)

Things to do:
- Alert personnel
- Ascertain damage
- Retrench to a Standby facility – if necessary
- Action BCP Support matrix/teams – as necessary
- Invoking Operational Procedures
- 3rd Party Suppliers

Operational Procedures:
- PAS recovery
- Office Systems recovery
- eMail recovery
- Network recovery
- Recovery of department specific systems

[1] For an up-to-date categorisation list, see appendix A

4.1 Organisation of Business Continuity Response and Recovery

The organisational backbone of ICT Business Continuity Planning at the Trust is the BCMT. In the event of a disaster affecting the Trust or its resources, the BCMT will respond in accordance with this Policy and will initiate specific actions for recovery. The BCMT is called into action under the authority of the Trust Board of Directors who have the responsibility for approving actions regarding Business Continuity Planning at the Trust.

4.2 Business Continuity Management Team (BCMT - ICT)

For the Business Continuity of the Trust's ICT Systems, three groups are key: Executive Board of Directors[2], the BCMT, and the Trust's ICT Support Teams. In the event of a disaster, the BCMT provides general support, while the ICT Support Teams are concerned with resources and tasks integral to running the specific functional areas.

This section provides general information about the organization of recovery efforts and the role of the BCMT. Part III of this document describes the BCMT and the responsibilities of each Trust Support Team in detail.

4.3 Disaster Recovery Plan (DCP)

This section describes the required responses to a disaster, or to a problem that could evolve into a disaster:

- Detect and determine a disaster condition
- Notify persons responsible for recovery
- Initiate the Trust's ICT Business Continuity Policy
- Activate the designated hot site - if necessary
- Disseminate Public Information
- Provide support services to aid recovery

Each subsection below identifies the organization(s) and/or position(s) responsible for each of these six responses.

4.4 Detection and Determination

The detection of an event which could result in a disaster affecting information processing systems at the Trust is the responsibility of ICT Services, or whoever first discovers or receives information about an emergency situation anywhere across the Trust.

4.5 Notification

The Duty 'bleep holder' will either:

- notify the ICT Services help desk, or;

[2] Trust IT Services Risk Assessment dated 26th August 2005

- use the ICT Business Continuity Callout List,

and then monitor the evolving situation.

4.6 Initiation of the Trust's ICT Business Continuity Policy

When a situation occurs that could result in interruption of processing of major information processing systems, the following people must be notified, where possible:

- ICT Services Manager
- ICT Systems and Development Manager
- ICT Infrastructure Manager
- ICT Programme Manager
- Telecommunications Manager
- Deputy Director of ICT
- Information Governance Manager (BCMT Coordinator)
- Head of Information
- Medical Records Manager(s)

4.7 Activation of a Designated Standby Facility

The responsibility for activating any of the designated standby facilities[3] or back-up resources is delegated to the Deputy Director of ICT. In their absence responsibility reverts to the nominated deputy and ICT Support Manager. As soon as possible after the occurrence, the Deputy Director of ICT, or the appointed deputy, determines the prognosis for recovery of the damaged functional area through consultation with the Information Governance Manager and the Damage Assessment Team, headed by Estates.

4.8 Dissemination of Public Information

The Communications Manager is responsible for directing all meetings and discussions with the news media and the public, and in conjunction with the Personnel Department, Trust personnel not actively participating in the recovery operation. In their absence, the responsibility reverts to the Duty Manager on call.

4.9 Provision of Support Services to Aid Recovery

During and following a disaster, Trust Support Teams are responsible for aiding local departmental managers. They operate under the direction of the BCMT through the Recovery Coordinator (the Information Governance Manager).

4.10 Business Continuity Strategy

The Business Continuity strategy explained below pertains specifically to a disaster disabling the main Computer Rooms at the DRI and Bassetlaw Hospitals. These functional areas provide mainframe computer and major

[3] For an up-to-date list of designated standby facilities, see appendix B

server support to the Trust's administrative applications and IP telephony requirements etc. Especially at risk are the 'critical applications', i.e. those designated as Category I systems. The ICT Support Teams provide for recovering the capacity to support these critical applications at the earliest opportunity. Summarizing the provisions of the Policy, subsections below explain the context in which the Trust's Business Continuity Policy operates. The Business Continuity Policy complements the strategies for restoring the data processing capabilities normally provided by ICT Services.

4.11 Disaster Recovery Strategy

This section addresses three phases of disaster recovery:

- Emergency
- Backup
- Recovery

Strategies for accomplishing each of these phases are described below. It should be noted that the subsection describing the emergency phase applies equally to a disaster any building across the Trust affecting a designated 'critical' system.

4.12 Emergency Phase

The emergency phase begins with the initial response to a disaster. During this phase, the existing emergency plans and procedures direct efforts to protect life and property, the primary goal of initial response. This will necessarily include Patients, the Public and Members of Staff. Security over the area is established as local support services such as the Police and Fire Departments are enlisted through existing mechanisms. The Duty Manager is alerted by pager and begins to monitor the situation.

If the emergency situation appears to affect one of the main Computer Rooms (or other critical facility or service), either through damage to data processing or support facilities, or if access to the facility is prohibited. The Duty manager will closely monitor the event, notifying BCMT personnel as required to assist in damage assessment. Once access to the facility is permitted, an assessment of the damage is made to determine the estimated length of the outage.

	BROAD CLASSIFICATION OF RISK	SERVICE IMPACT	CONTINUITY MEASURES	ACTION REQUIRED TO REDUCE RISK LIKELIHOOD OR IMPACT
1	Loss of electrical power	Inability to operate critical systems. Likely duration of disruption: 1 hour to 3 days.	Manual operations. Refer to Estates Dept. plan for power continuity	Improvement to emergency power provision
2	Serious environmental damage to computer room(s)	Inability to provide critical services. Likely duration of disruption: 2 weeks to 8 weeks depending on severity	Manual operations. Liaison with Estates and suppliers re: recovery plan.	Reduce risks to computer room(s) by strengthening physical and environmental security
3	Denial of service attack by: - Serious software / system malfunction - Serious Virus/Trojan Code/Worms	Most likely to affect office systems as a minimum. Could prevent access to some patient based applications. Likely duration of disruption: 4 hours to 5 days	Possible provision of very limited access to patient systems - otherwise manual operations.	Service improvements are being made in line with Connecting for Health (N3) requirements
4	Serious loss of staff (e.g. sickness / strike) or loss of physical access to computer rooms (e.g. terrorist activity etc.)	Impact will increase over time resulting in unpredictable degradation of the service. Likely duration: up to 7 days	Prepare for manual operations.	Further planning to be undertaken to mitigate impact of this category of threat.

NOTES
1. For loss of availability of patient based systems such as PAS, the updating of information when systems become available again will be an additional factor for service areas to include in their plans
2. See additional matrices for more detailed information on impact and locations affected.

If access to the facility is precluded, then the estimate includes the time until the effect of the disaster on the facility can be evaluated.

The BCMT remains active until recovery is complete to ensure that the Trust will be ready in the event the situation changes.

4.13 Back-up Phase

The back-up phase begins with the initiation of the appropriate Policy(s) for outages caused by a major disaster. In the initial stage of the back-up phase, the goal is to resume processing 'critical applications'. Processing will resume either at the main Computer Room or at the designated standby facility, depending on the results of the assessment of damage to equipment and the physical structure of the building.

In the back-up phase, the initial standby facility must support critical (Category I) applications and as many Category II applications as resources and time permits. During this period, a reduced service resumes, up to the capacity of the standby facility. Within this period, a main Computer Room or alternative facility will be returned to full operational status.

4.14 Recovery Phase

The time required for recovery of the functional area and the eventual restoration of normal services depends on the damage caused by the disaster. The time frame for recovery can vary from several days to several months. In either case, the recovery process begins immediately after the disaster and takes place in parallel with back-up operations at the designated standby facility. The primary goal is to restore normal operations as soon as possible.

5. TEAM DESCRIPTIONS AND RESPONSIBILITIES

The ICT Business Continuity Management Team (BCMT) is composed of Senior Trust Managers. The following is a list of each position on the BCMT, and a brief overview of each member's responsibilities:

- **Deputy Director of ICT -** Acts as Chair of the BCMT and as link-person to the Trust Management Board. Provides for audit support during the emergency. Makes recommendations on changes to the normal control procedures necessitated by the recovery process.

- **Information Governance Manager** - As Coordinator of the BCMT, with assistance from ICT Managers, provides liaison between the Trust's operational and management teams and the ICT support teams in affected areas. Also responsible for ongoing maintenance, training and testing of the Trust's Business Continuity Policy with ICT Services. Coordinates the Trust support teams under the auspices of the BCMT.

- **ICT Services Manager** - As Co-Coordinator of the BCMT, provides liaison between the Trust's operational and management teams and the ICT Support Teams in affected areas. Responsible for purchase of replacement Assets and for maintenance of the Asset register. Provides technical support for ALL Computing Facilities and other distributed ICT Services and Networks.

- **Finance Director** - Coordinates support for data processing resources at the main data centres and any designated recovery sites. Provides liaison with insurers and claims adjusters.

- **Telecommunications Manager** - Provides alternate voice and data communications capability in the event that normal telecommunication lines and equipment are disrupted by the disaster. Evaluates the requirements and selects appropriate means of backing up the Trust's telecommunications network.

- **Security Manager** - Provides for physical security and emergency support to affected areas and for notification mechanisms for problems that are or could be disasters. Extends a security perimeter around the functional area affected by the disaster.

- **Director of Estates** - Coordinates all services for the restoration of plumbing, electrical, and other support systems as well as structural integrity. Assesses damage and makes a prognosis for occupancy of any structures affected by the disaster.

- **Communications Manager** - Communicates with the news media, public, staff, faculty, and student body who are not involved in the recovery operation.

- **Director of Human Resources** - Provides support for human resources elements of recovery and staff notification through the emergency broadcast service. Provides network support for Administrative and Academic Computing and other distributed services and networks. Provides audit support during the emergency.

- **Risk Manager** - Coordinates risk reduction and avoidance activities and emergency response with the BCMT.

- **Emergency Response Team** - This team, headed by the Director of Estates, provides the initial response to the majority of Trust emergencies[4].

Trust Support Teams:

Under the overall direction of the BCMT, Trust Support Teams provide support to assist a functional area's recovery. These teams, described below, work in conjunction with personnel in the area affected by the problem condition to restore services and provide assistance at the Trust level. In many cases, these support teams have as their normal responsibility the provision of these support services. This support is generally documented in a procedure manual. The Business Continuity Policy is an adjunct to that documentation and highlights, in particular, the interfaces between the Trust level service and the individual department's operational requirements. In cases where the documentation in this Policy and the department's documents differ, the department's documentation has precedence. It will be a requirement that Depts, Clinical areas etc to have there own Business Continuity and Disaster Recovery Policies and Plans.

- **Damage Assessment/Salvage Team** - Lead by Estates and activated during the initial stage of an emergency, the team reports directly to the BCMT, evaluates the initial status of the damaged functional area, and estimates both the time to reoccupy the facility and the salvageability of the remaining equipment. This team draws members from Estates, ICT Services, Fire and Health & Safety Officers, Security Manager, Telecommunications Systems team, local managers of the affected area as well as appropriate vendors supporting the environment.

- **Following the assessment of damage**, the team is responsible for salvaging equipment, data and supplies following a disaster; identifying which resources remain; and determining their future utilization in rebuilding the data centre and recovery from the disaster. The members of the Damage Assessment Team become the Salvage Team.

- **Transportation Team** - Operations Department will be responsible for transporting resources, personnel, equipment, and materials to back-up sites as necessary. This team draws members from two organizations: Information Systems and Estates - including Security, Fire and Health & Safety Personnel as necessary.

- **Public Information** - The interface with the media, the general public and patients and staff who are not participating in the recovery process is handled by the Trust's Communications Office, working closely with the Personnel Department.

- **The Telecommunications Manager** (with assistance of ICT Infrastructure Manager) is responsible for establishing voice and data communications between the affected site and the remainder of the campus.

[4] For MAJAX Emergencies the Response team is led by the Bassetlaw Hospital Manager

Damage Assessment/Salvage

- To report to the BCMT, within two to four hours after access to the facility is permitted, on the extent of the damage to the affected site, and to make recommendations to the BCMT regarding possible reactivation and/or relocation of data centre or user operations. Following assessment of the damage, the team is then responsible for salvage operations in the area affected.

- Headed by the Operations Director or Deputy and activated during the initial stage of an emergency, the team reports directly to the BCMT, evaluates the initial status of the damaged functional area, and estimates the time to reoccupy the facility and the salvageability of the remaining equipment.

- During an emergency situation, the Operations Director will take operational responsibility for implementation of damage assessment. This team draws members from Estates and ICT Support Services and from Senior Managers of the affected area. Following assessment, the team is responsible for salvaging equipment, data, and supplies following a disaster; identifying which resources remain; and determining their future utilization in rebuilding the data centre and recovery from the disaster.

- The Damage Assessment/Salvage Team will interface with members of the Trust Management Board, Security and Information Systems Managers, including vendor and insurance representatives, to keep abreast of new equipment, physical structures, and other factors relating to recovery.

- Identification of all emergency equipment is to be kept current. An annual report will be stored off-site. The listing will show all current information. Configuration diagrams will also be available. Estates will maintain emergency equipment, including portable lighting, hard hats, boots, portable two-way radios, floor Policy's and equipment layouts.
    - A listing of all vendor sales personnel, customer engineers and regional sales and engineering offices is to be kept and reviewed quarterly. Names, addresses and phone numbers (normal, home, and emergency) are also to be kept.

Trust Security Teams

- To provide for all facets of a positive security and safety posture, to assure that proper protection and safeguards are afforded all Patients, the Public and Trust employees and for Trust assets at both the damaged and backup sites.

- The team will consist of the Trust Security Manager and appropriate support staff. The team will report through the Trust Security Manager who is a member of the BCMT.

- The Trust Security Manager will interface with the following teams or organizational units, relative to security and safety requirements:

- HR & Personnel, Estates, Fire and Health & Safety Officers, Environmental Medical Services, Occupational Health, Communications Office, Other appropriate departments as required

- Identify the number of Security personnel needed to provide physical security protection of both the damaged and backup sites.

- Identify the type of equipment needed by Security personnel in the performance of their assigned duties. Coordinate and arrange for additional security equipment and manpower, as applicable, if needed. Identify and provide security protection required for the transport of confidential information to and from both off-site and backup sites.

- Periodically review the level of security needed at both the damaged and backup sites.

Communications Office - Public Information

The most difficult time to maintain good public relations is when there is an accident or emergency. Public relations planning is required so that when an emergency arises, inquiries from the news media, friends and relatives of patients and staff can be handled effectively. While we cannot expect to turn a bad situation into a good one, we can assist in making sure facts presented to the public are accurate and as positive as possible given the situation.

It is in our best interest to cooperate with the media as much as possible, so that they will not be forced to resort to unreliable sources to get information that could be untrue and more damaging to the Trust than the facts.

Therefore, it is the policy of the Trust in time of emergency, to:

- Have the Communications Office serve as the authorized spokesperson for the Trust. All public information must be coordinated and disseminated by their staff.

- Refrain from releasing information on personnel casualties until families have been notified. Once families have been notified, names of those personnel should be released quickly to alleviate the fears of relatives of others.

- Provide factual information to the press and authorities as quickly as facts have been verified, and use every means of communications available to offset rumours and misstatements.

- Avoid speculating on anything that is not positively verified, including cause of accident, damage estimates, losses, etc. (Fire Officials normally release their own damage estimates.)
- Emphasize positive steps taken by the Trust to handle the emergency and its effects.
- Situations calling for implementation of the Major Incident Policy may include, but are not limited to:

    - Systems malfunctions disrupting the normal course of operations.
    - Accidents, particularly when personal injury results.
    - Natural disasters, such as fires, floods, unusually high winds and explosions.
    - Civil disorders, such as riots and sabotage.

- Executive death.
- Scandal, including embezzlement and misuse of funds.
- Major litigation initiated by or against the Trust.

The Communications Manager, a member of the BCMT, will act as the Public Information Officer for the Trust. In their absence the responsibility will revert to the Duty Manager on the scene.

The Communications Office will be the interface between the Trust and the public or news media. Copies of all status reports to the BCMT or Trust Management Board will be forwarded to the Communications Manager for potential value in information distribution for good public relations. They will work with the Personnel Department in dissemination of information to staff.

Existing relationships with local media will be utilized to notify the public of emergency and recovery status. The Communications Manager will maintain up-to-date contact information for the media and other required parties.

A facility will be identified to be used as a pressroom. Arrangements will be made to provide the necessary equipment and support services for the press. Coordination with the Telecommunications Team for additional voice communication, if required, will also be made.

Insurance

To provide for all facets of insurance coverage before and after a disaster and to ensure that the recovery action is taken in such a way as to assure a prompt and fair recovery from our insurance carriers.

Determine needs for insurance coverage. Identify the coverage required for hardware, media, media recovery, liability and extra expense. Prepare procedure outlining recommended steps to be followed by Damage Assessment/Salvage Team during initial stage of disaster and list appropriate contacts.

Arrange for availability of both still and video recording equipment to record the damage.

Ensure that an equipment inventory is available, to include model and serial number of all devices.

Evaluate all new products and services offered by the Trust for potential liability in the event of a disaster.

Telecommunications

To provide voice and data communications to support critical functions. Restore damaged lines and equipment.

The team will consist of appropriate Telecommunications Systems staff and ICT Infrastructure staff. Telecommunications Systems will also coordinate with and supervise outside contractors as necessary. The team will report through the Telecommunications Manager, who is a member of the BCMT.

The Telecommunications Systems team will interface with the following teams or organizational units, relative to telecommunications requirements:

- Estates
- Security
- ICT Services and ICT Infrastructure
- Other Information Systems departments as necessary
- Other Trust departments requiring emergency telecommunications
- Outside contractors and service providers as necessary

Provide critical voice communications services in the event that normal telecommunications lines and equipment are disrupted or relocation of personnel is necessary. Consult with outside contractors and service providers to ensure that replacement equipment and materials are available for timely delivery and installation.

6. EDUCATION & TRAINING

Business Continuity Training is provided centrally by the Trust.

7. MONITORING COMPLIANCE & EFFECTIVENESS

The ICT Services Department with the ICT Risk Management Group carries out desk-top educational scenarios to emulate possible disasters and to test and review the current policy and its associated Standard Operational Procedures (SOPs).

8. AUDIT

Internal Audit play an important role in the scenario setting for Section 8. The Internal Audit Services carry out an agreed and 'risk based' annual audit plan.

9. ASSOCIATED DOCUMENTATION

CORP/ICT 2 - ICT Security & Confidentiality Policy

BS7799 Part 1, ISO17799:2005, ISO/ISE 27001

DH: Information Governance Toolkit

APPENDIX A

Asset Function Categorisation

- Category 1 – Critical Functions

  - Trust LAN/WAN
  - Trust Integration Engine (TIE)
  - PAS/CRS
  - Radiology
  - Pathology
  - Drug Prescription and Administration (JAC)
  - Order Communications and Results Reporting (ICE)
  - Theatres
  - A&E (EDIS)
  - N3 (NHS Network v3)
  - X-Ray (Picture Archiving & Communications - PACS)
  - Trust eMail
  - Medical Records
  - IP Telephony Services and Applications

- Category 2 – Essential Functions

  - Electronic Staff Record (ESR)
  - Office Systems
  - Ambulance Systems
  - Internet (World-wide Web)
  - Solidus Contact Centres (Med Recs, Pathology Results, GP OOH's)

- Category 3 – Necessary Functions

  - Clinic Based systems
  - Audit systems
  - Trust Intranet

- Category 4 – Desirable Functions

  - Training systems
  - Car Parking

APPENDIX B

List of Designated Standby Facilities:

- DRI
    - ICT Department
    - Main Computer Room
    - Pathology Computer Room
- Bassetlaw
    - ICT Department
    - Cost Office
    - Main Computer Room
- Montagu
    - Boardroom
    - tbn