1. Approval and Authorisation

Completion of the following signature blocks signifies the review and approval of this Process (signed copy held in safe)

Name	Job Title	Signature	Date
Authored by:- <Name>	Technical Support Officer		
Approved by:- <Name>	Information Security Officer		
Authorised by:- <Name>	Director of Finance & IT		

2. Change History

Version	Date	Reason
Draft 1.0		First draft for comments
Version 1.0		First Version
Version 1.1		Amendment to ISCIG “voting” to minimum of 3 to approve.
Version 1.2		Removal of “user survey” material. Incorporation of change controls along lines of major & minor changes.

3. Contents

4. Abbreviations & Definitions Used in this Report

Systems – operating systems and/or application systems and/or hardware

System Manager – the person in IT responsible for a system.

Owner – the person in the user community who has overall control over use, change requests and day-to-day user running of the system (eg decide what type of information goes on the system or who has access to what areas of the application/data etc.).

CRF – Change Record Form (Appendix 1).

ISCIG – Information Systems Change Implementation Group.

Requester – the person requesting or initiating the change.

Developer – the member of staff in IT Operations or IT Development who will undertake the technical aspects of the change.

(Forms in Appendix 1 constitutes part of this document.)

5. Introduction

The aim of this document is to put in place procedures that minimise the risk of damage to the Trust's information systems, data and business that may come from changes to its computer systems.

The document covers procedures to be adopted when any change is made to the Trust's I.T systems in the following areas: operating systems, application systems and hardware. It initiates a new body within the Trust which will have overall control of all changes made to the system

It will cover all aspects of change from request to implementation – including fall-back options where a change has failed. This document is mainly about the IMPLEMENTATION of changes so it will cover, minimally, the change request from a user to a developer testing prior to implementation.

6. Operational Change Control Process

6.1 Overview

The operational change control process covers change initiation of change, control of change, record keeping, decision making for all aspects of change on the Trust's corporate information systems on computer. The process have been devised to allow minimum time impact on the actual changes themselves – that is the process should not, in itself, slow down the start or pace of a change. There are two processes – one for projects and large changes (the Major Change Process) and the other for smaller changes (the Minor Change Process). Each process is described in the sections that follow.

6.2 Record Keeping And Auditing Of Changes To Systems

An audit trail will be kept. Each change will have a form which will record progress at every stage. The form will be the basis of the final implementation change control decisions process.

The Major Change Record Form (ACR) (Appendix A), and the Minor Change Record Form (ICR) (Appendix 3) both form part of the documentation of this section.

6.3 Test Systems

Wherever possible change & implementation work should be tested on a test system which is not a part of the live, production systems. The test systems should be as close to the live system in its configuration as possible. Changes should be tested on a test system, if possible, prior to a change implementation request being made.

6.4 Who Makes Change Control Decisions?

The decision as to whether a change is deemed to be a Major Change or a Minor Change will be taken by the IT Operations Manager.

Major Change Control
The decision as to whether a change will be implemented on to a live system will be taken by a group known as the Information Systems Change Implementation Group (ISCIG).

This group will consist of at least three of the following :

1 The Owner of the system

2 The System Manager

3 The IT Operations Manager

4 The Desktop Systems Development Manager

5 The Director of Finance & IT

Minor Change Control
For web site changes the people who take the decisions on whether change are as detailed in Appendix 2.

For all other changes the group which will give approval consists of:

1 The IT Operations Manager;

2 The System Owner and

3 The Developer.

6.5 The Change Implementation Process

It is envisaged that the main areas of the Trust's computer-based information systems in which change will be made (and the Change Implementation Process will be used) are infrastructure (controlled by the Desktop Systems Development Manager [DSDM]) and web-development (controlled by the Web Development Team Leader [WDTL]). (The classifications of different types of web development work is defined in Appendix 2 of this document.)

There are two different levels of change which affect the Trust's computer-based information systems, these can be classified as follows:

a) Major changes to systems (**the Major Change Implementation Process**). This process covers changes which will have a major effect on the information systems – for example: installing a brand new system (hardware, software etc.); replacing an existing system (hardware and/or software); upgrading operating systems or GUIs to new versions (for example Windows NT to Windows XP). It is to be used to implement whole new projects.

b) Minor changes to existing systems (**the Minor Change Implementation Process**). This process covers minor changes to systems – every change which is not covered by the Major Change Implementation Process (see section 6.5a). An example of such a change would be the normal, every day web-development work undertaken by the . Web Development Team.

The choice of process for each piece of work will be made by the IT Operations Manager.

6.6 The Major Change Implementation Process

The process involves:

1 The steps in part A of the CRF will be completed by the Requester, the Owner and the Developer.

2 Part B of the CRF will be filled in by the Requester, the Owner and the Developer and passed to all members of the ISCIG (via the Helpdesk).

3 The CRF will be approved (or otherwise) by at least three members of the ISCIG by a given date.

4 Once the ISCIG has made a decision it will be communicated to the Requester, the Owner and the Developer.

5 If the change is approved then the Requester, the Owner or the Developer will request the IT Operations Manager or Desktop Systems Development Manager to arrange for the implementation of the change.

6 Prior to implementing the change the system(s) will be safe-guarded by taking steps to provide a "fall back" position if needed [eg by making a back-up of the system(s) involved].

7 Once implemented the change must be monitored by the Requester, the Owner, the Developer, the IT Operations Manager and the Desktop Systems Development Manager to ensure that there are no problems. If problems occur which require invoking the "fall back" procedure on the CRF. The IT Operations Manager or Desktop Systems Development Manager will arrange this, having informed all parties involved (ie the Requester, the Owner, the Developer and users of the system). ISCIG members will be informed by e-mail.

8 If the ISCIG does NOT approve the change they will provide feed-back to the Requester, the Owner and the Developer in order that they may take appropriate action (eg change their submission or abandon it etc.).

9 Once implemented the relevant technical, operating & user documentation will be updated as appropriate. This is the responsibility of the Owner and the Developer.

10 If appropriate changes to the Business Continuity plan must be made. This will be organised by the IT Security Officer.

11 If necessary, changes which affect systems which are shared by or are accessed through the NHS Logistics Authority should be communicated to the Authority in case changes affect the shared services. Liaison should take place, too, to ensure that any changes to Authority systems which are used by the Trust are communicated to the IT Operations Manager and the Desktop Systems Development Manager so that they may review impact upon systems run by the Trust.

12 The complete ACR form will be kept by the IT Helpdesk at Reading as a record of the change for future reference.

6.7 The Minor Change Implementation Process

1 The designation of a piece of work as a Minor Change will be made by the IT Operations Manager.

2 The ICR form should be completed by the Requester , who should give the following information:

a) The category (whether the change is to hardware, software (including operating systems & GUIs), a web-site, the National Database or “other”).

b) A brief description of the change required.

Later on the member of staff who makes the change should also note here any “intermediate” changes that needed to be done to make the change work correctly etc. – for example, if a patch is required to an operating system in order to make a new version of a web-browser work then the incorporation of that operating system patch should be noted here.

c) The date by which the change is required (live).

3 In the case of changes to web pages the approval procedure outlined in Appendix 2 is followed.

In all other cases approval will be given by the IT Operations Manager.

4 In all cases, the officer responsible for making the change “live” will complete the relevant sections of the ICR for,m (ie “Completed”, “Set Live” and “Live Date”.

5 The complete ACR form will be kept by the IT Helpdesk at Reading as a record of the change for future reference.

6.8 Additional Guidance For Developers And The ISCIG

1 It must be established that the support plan and budget will cover reviews and testing of changes.

2 The Desktop Systems Development Manager and the IT Operations Manager should check that application control & integrity procedures are reviewed in light of the changes.

3 Changes to vendor-supplied software packages should NOT be allowed except in exceptional circumstances. In which case the vendor should either consent to the change or be allowed to make the change as either a standard update or a bespoke change.

Appendix 1: Major Change Record Form

Change record form Reference: ACR ***This form constitutes the formal log of a change and must be kept as a record of that changes history.***
Reference number:
Part A: **(In order for Part B to be submitted this part must be complete)**
1. Requester name: **2. Approved by (owner):** **3. Change required to: Operating System/Application System/Hardware** (Delete as applicable)
4. Details of change:
5. Developer acceptance: y/n **6. Test version accepted by Requester: y/n**
PART B: (In order for implementation to be authorised PART B must be complete.)
7. Description of change to system (in general, not technical terms)
8. Why is the change needed?
9. What are the advantages of the change?
10. What are the risks of implementing this change?
11. What are the disadvantages (if any) to the change?
12. What are the risks of NOT implementing this change?

13. What is the potential effect on the service and users (include support/maintenance costs and whether approved or not; are extra licences needed?)
14. Timetable for implementation: What date and time is change required live? Do users need to be "off the system" when the change is implemented? y/n Do they need to be totally logged off from all systems when change is implemented? y/n
15. What resource and effort are involved in change implementation?
16. In case of failure once the change has gone live what is the "fall back" procedure? Give full details – step by step possible.
17. To be filled in by ISCIG member: Name: Date: Approved: y/n Need more information:
If more information needed, what information do you need?
18. Implemented: y/n **19. Notification of implementation:** Owner (to notify users if applicable) Desktop Systems Development Manager (to arrange physical implementation) Developer (if applicable) **20. Documentation amended** Technical y/n/not applicable Operating y/n/not applicable User y/n/not applicable
21. If applicable, Xxxxxxxxxx Authority informed of change y/n/not applicable

Appendix 2: Web development approval processes

There are four such processes, each of which has a slightly different hierarchy of approval. Each of these processes are classified as minor changes and thus would follow the Minor Change Implementation Process. The four web-approval processes are outlined below:

1 **No significant change** – for example, a new price list. Such work would be distributed by and approved by the Web Development Team Leader..

2 **Significant change** – for example a user with already existing area on the web site would like a further ten pages adding to that area. Such work would be approved by the Web Master when completed.

3 **Material seen in advance** for users. The Web Development Team Leader will analyse and schedule the work and pass back the finished work to the Web Master for approval.

4 **Extremely urgent, large projects at an Trust level**. The IT Operations Manager will discuss the user requirements with the Web Master. The work will be passed to the Web Development Team Leader who will produce a timescale for the work and arrange for it to be done. Once completed the work will be approved by the IT Operations Manager and the Web Master.

Appendix 3: Minor Change Record Form

Minor Change Record Form	Ref: ICR

Change Reference No: ICR | **Request Date:**

Details of change:

Category: Hardware/Software/Web/National Database/Other - Details:

Description:

(Note any relevant intermediate changes made while making this change, here or overleaf.)

Date Required: **Timescale:** **Completed:**

Approved: **Approval Date:**

Approved by:
IT Operations Manager:
Owner:
Developer:

Signature

Set Live:

Live Date: