

Confidentiality Audit Procedure

Version	1.0
Status	Ratified
Author/Lead	Information Governance & Data Protection Officer
Directorate	Finance and Performance
Ratified By	ICT & Information Governance Programme Group
Implementation Date	March 2011
Date of Last Review Date	February 2011
Date of Next Review	February 2012
Target Audience	All Staff

To be read with:

- Confidentiality and Data Protection Policy
- Information Governance Policy
- Information Risk Policy
- Incident Reporting and Management Policy
- Serious Incidents Policy

“The PCT incorporates and support the human rights of the individual as set out in the European Convention on Human Rights and the Human Rights Act 1998”

Version Control Record

Version	Description of Change(s)	Reason for Change	Author	Date
0.0.1	N/A	New document	Information Governance & Data Protection Officer	28/10/2010
0.1	Added reporting of unauthorised release of confidential information to breach monitor list.	Comments from Acting Head of Governance	Information Governance & Data Protection Officer	14/12/2010
0.2	Minor grammatical changes	Comments from Business Systems Manager	Information Governance & Data Protection Officer	07/02/2011
1.0	Ratified	Ratification	Information Governance & Data Protection Officer	23/03/2011

Table of Contents

1.	Introduction	4
2.	Purpose.....	4
3.	Scope.....	4
4.	Monitoring Access to Confidential Information	5
5.	Responsibilities	5
6.	Disciplinary Procedures	6
	Appendix 1 - Monitoring and Review	7
	Appendix 2 - Procedure Ratification and Publication	7
	Appendix 3 - Assurance Form	8

1. Introduction

- 1.1 Good practice requires that all organisations that handle personal information put in place control mechanisms to manage and safeguard confidentiality, including mechanisms for highlighting problems such as incidents, complaints and alerts.
- 1.2 Organisations should have processes to highlight actual or potential confidentiality breaches in their systems, particularly where person identifiable information is held.
- 1.3 This procedure has been developed to provide assurances to the PCT that appropriate processes will be followed by PCT staff in accordance with Trust Policy.

2. Purpose

- 2.1 The purpose of this procedure is to ensure that processes are in place to highlight actual or potential confidentiality breaches in systems.

3. Scope

- 3.1 This policy applies to all employees of NHS Brent and Brent Community Services (BCS), including contracted and temporary staff.
- 3.2 This procedure covers both electronic and manual (paper) systems.

4. Monitoring Access to Confidential Information

- 4.1 In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis.
- 4.2 Monitoring will be carried out by the ICT and Information Governance Programme Group so that irregularities regarding access to confidential information can be identified, and reported to the Caldicott Guardian, Senior Information Risk Owner and Board where necessary.
- 4.3 The ICT and Information Governance Programme Group may decide actions to be taken to address the situation, through the implementation of additional controls or other remedial action as necessary.
- 4.4 Actual or potential breaches of confidentiality should immediately be reported to the Caldicott Guardian via Datix, the PCT's incident management system.
- 4.5 Such incidents should be reported to the ICT and Information Governance Programme Group for consideration.
- 4.6 Should unauthorised access to confidential information be gained by any individual, this will be dealt with in accordance with the Trust's disciplinary procedures.

5. Responsibilities

- 5.1 **All Staff**
If staff discover a breach in confidentiality, they should report it via the PCT's incident management system, Datix.
- When reporting a confidentiality breach staff must observe the following policies:
- Incident Reporting and Management Policy
 - Serious Incidents Policy
- 5.2 **Information Governance & Data Protection Officer**
The Information Governance & Data Protection Officer will provide audit reports to the ICT & IG Programme Group of confidentiality breaches and investigations.
- The Information Governance & Data Protection Officer will provide advice or participate in investigations of confidentiality events.
- 5.3 **Caldicott Guardian**
The Caldicott Guardian will be informed of confidentiality breaches, and act accordingly.

5.4 **Senior Information Risk Owner**

The Senior Information Risk Owner will be informed of confidentiality breaches, and report to the Board where appropriate.

5.5 **ICT & Information Governance Programme Group**

The ICT & IG Programme Group will periodically monitor confidentiality breaches, including but not limited to:

- Failed attempts to access confidential information.
- Repeated attempts to access confidential information.
- Successful access of confidential information by unauthorised persons.
- Evidence of shared login sessions/passwords, including Registration Authority Smartcards.
- Unauthorised release of confidential information.

The ICT & IG Programme Group will also review the outcome of investigations into confidentiality breaches.

6. Disciplinary Procedures

- 6.1 All suspected breaches of this policy will be investigated and may be subject to the Trust's formal disciplinary procedures. Serious breaches may result in immediate suspension and/or termination of contract, under the PCT Performance and Conduct Policy and the Serious Incident Policy.

Appendix 1 - Monitoring and Review

This Procedure will be reviewed once a year by the ICT & IG Programme Group. Auditing of this document should be done at least every two years based on monitoring the effectiveness of the Procedure. The Assurance Form (Appendix 3) will be used by Managers to document staff understanding of the Procedure.

Appendix 2 - Procedure Ratification and Publication

Procedure Title (including version)		Date
Confidentiality Audit Procedure 1.0		23 March 2011
Reason for Submission (Please Tick)		
Scheduled Review <input type="checkbox"/>	New Procedure	<input checked="" type="checkbox"/>
Urgent Amendments <input type="checkbox"/> (Please specify)	Other	<input type="checkbox"/>
<input type="text"/>		
Purpose of the Procedure		
This procedure outlines the processes in place to discover whether confidentiality has been breached.		
Supporting Evidence Please state list of reviewers/stakeholders and their job title (use a separate sheet if required) along with evidence of their participation in the review/creation of the procedure.		
Reviewers: <ul style="list-style-type: none"> • Business Systems Manager • Head of Governance • Head of Corporate Affairs 		
Procedure Approval		
Name:	Chair of ICT & IG Programme Group	
Signature:	Mark Easton	
Date:	23/03/2011	

