The Queen Elizabeth Hospital NHS
King's Lynn
NHS Foundation Trust

INFORMATION GOVERNANCE POLICY

Unique Reference / Version				
Primary Intranet Location	Policy Name	Version Number	Next Review month	Next review year
Information Management & Governance	Information Governance Policy	5.0	February	2014
Secondary Intranet Location				

Current Author	Phil Cottis
Author's Job Title	Information Governance & RA Manager
Department	IM&T
Ratifying Committee	Information Governance Committee
Ratified Date	13 February 2013
Review Date	13 February 2014
Owner	Barbara Cummings
Owner's Job Title	Director of Planning & Performance

It is the responsibility of the staff member accessing this document to ensure that they are always reading the most up to date version. This will always be the version on the intranet

Related Policies	Information Governance Strategy Management of Adverse Events Policy and Procedure Information Security Policy

Stakeholders	Information Governance Committee Non-Clinical Governance Committee

Version	Date	Author	Author's Job Title	Changes
V3	December 2010	Nic McCullagh	Information Governance Manager	Annual review
V4	February 2012	Phil Cottis	Information Governance & RA Manager	Annual review
V5	December 2012	Phil Cottis	Information Governance & RA Manager	Annual review and format change

Short Description

The purpose of this policy is to provide details of the framework for implementation of the Information Governance (IG) strategy to enable the Trust to meet its responsibilities for the management of information assets and resources.

Key words

Information, Security, Confidentiality, Sharing, Caldicott

INFORMATION GOVERNANCE POLICY

CONTENTS

INFORMATION GOVERNANCE POLICY

1 INTRODUCTION

1.1 Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

1.2 It is of paramount importance to ensure that information is effectively and efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

1.3 The policy is intended to be fully consistent and compatible with the policies and practices throughout the NHS and the Trust strategy for Information Governance and is developed to achieve compliance to the Care Quality Commission Outcomes.

2 PURPOSE

2.1 The purpose of this policy is to provide details of the framework for implementation of the Information Governance (IG) strategy to enable the Trust to meet its responsibilities for the management of information assets and resources.

2.2 This policy applies to:

- All information used by the Trust;
- All information systems managed by the Trust;
- Any individual using information 'owned' by the Trust; and
- Any individual requiring access to information 'owned' by the Trust.

3 DEFINITIONS

3.1 **Breach of Confidentiality**
A breach of confidentiality is the unauthorized disclosure of personal information provided in confidence.

3.2 **Confidential Information**
Confidential information can be anything that relates to patients, staff or any other information (such as contracts, tenders etc) held in any form (such as paper or other forms like electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on portable devices such as laptops, PDAs, BlackBerrys, mobile telephones) or even passed by word of mouth. Person identifiable information is anything that contains the means to identify an individual.

3.3 **Disclosure**
This is the divulging or provision of access to data.

3.4 Patient identifiable Information

Key identifiable information includes:

- Patient's name, address, full post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of patients;
- NHS number and local patient identifiable codes;
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

3.5 Public Interest

Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.

3.6 Sensitive Data

Data held about an individual which contains both personal and sensitive information. There are only seven types of information detailed in the Data Protection Act 1998 that are deemed as sensitive:

- Racial or ethnic origin;
- Religious or other beliefs;
- Political opinions;
- Trade union membership;
- Physical or mental health;
- Sexual life; and
- Criminal proceedings or convictions.

4 RESPONSIBILITIES

4.1 Chief Executive

The Chief Executive is the accountable officer responsible for the management of the Trust and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Maintaining confidentiality is pivotal to the Trust being able to supply a first class confidential service that provides the highest quality patient care. The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 Senior Information Risk Owner (SIRO)

The Trust has appointed the Director of Planning & Performance as Senior Information Risk Owner (SIRO). The SIRO will act as an advocate for information risk on the Board and in internal discussions will provide written advice to the Accountable Officer on the content of their annual Statement of Internal Control in regard to information risk.

4.3 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The

Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

4.4 **Information Governance Committee**

The Information Governance Committee is responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

4.5 **Information Governance & RA Manager**

The Information Governance & RA Manager is responsible for advising on strategic direction, the development of policy and guidance for the Trust, and also operational support to the Trust.

4.6 **Trust Managers**

It is the responsibility of Executive Directors, Divisional Managers, Heads of Departments, Divisional Chief Nurses, Matrons and ward sisters/charge nurses to ensure the implementation of policies throughout their areas of responsibility. Managers should also react in an appropriate manner when informed of instances where behaviour is not in accordance with the policy that is set out herein.

4.7 **All Staff**

All employees and anyone working on behalf of the Trust, involved in the receipt, handling or communication of person identifiable information, must adhere to this policy to support the reputation of the Trust and where relevant of their profession. Everyone has a duty to respect a data subjects rights to confidentiality.

5 INFORMATION GOVERNANCE AIMS

5.1 The Trust's Information Governance aims are to:

- Hold information securely and confidentially;
- Obtain information fairly and efficiently;
- Record information accurately and reliably;
- Use information effectively and ethically;
- Share information appropriately and lawfully; and
- Encourage best practice.

6 INFORMATION GOVERNANCE PRINCIPLES

6.1 The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

6.2 The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

6.3 The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes.

7 LEGAL AND REGULATORY FRAMEWORK

7.1 There are a number of legal obligations placed upon the Trust for the use and security of person identifiable data.

7.2 There are requirements to appropriately disclose information when required.

7.3 There is an NHS regulatory and performance framework for the management of information.

7.4 There are NHS Codes of Conduct for the use of information.

7.5 There are Codes of Practice and operating procedures adopted by the NHS.

7.6 Appendix 1 provides further details of the legal and regulatory framework.

8 RESPONSIBILITIES OF THE TRUST

8.1 All information used in the NHS is subject to handling by individuals and it is necessary for these individuals to be clear about their responsibilities and for the Trust to provide and support appropriate education and training.

8.2 The Trust must ensure legal requirements are met.

8.3 The Trust must make arrangements to meet the performance assessment requirements of the Department of Health Information Governance Toolkit.

8.4 To manage its obligations, the Trust will issue and support standards, policies and procedures ensuring information is held, obtained, recorded, used and shared correctly.

8.5 The Trust will continue to report on the management of information risks in the statement of internal controls and to include details of data loss and confidentiality breach incidents in annual reports.

8.6 The Trust will ensure an Information Governance audit, utilising the centrally provided audit methodology, is included within the internal auditor's work plan.

9 RESPONSIBILITIES OF USERS

9.1 Users of information must:

- Be aware of their responsibilities, both legal and other, and that failure to comply may result in disciplinary action;

- Comply with policies and procedures issued by the Trust, and be aware that failure to comply may result in disciplinary action;
- Work within the principles outlined in the Information Governance framework; and
- Undertake annual Information Governance training.

10 KEY ELEMENTS OF THE INFORMATION GOVERNANCE FRAMEWORK

10.1 Freedom of Information

- Non-confidential information about the Trust and its services will be available to the public through a variety of media;
- The Trust has established and will maintain policies to ensure compliance with the Freedom of Information Act;
- The Trust undertakes or commissions annual assessments and audits of its freedom of information policies and arrangements;
- Patients have ready access to information relating to their own health care, their options for treatment and their rights as patients;
- The Trust has clear procedures and arrangements for liaison with the press and broadcasting media; and
- The Trust has clear procedures and arrangements for handling queries from patients and the public.

10.2 Legal Compliance

- The Trust regards all identifiable personal information relating to patients as confidential;
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements;
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise;
- The Trust has established and will maintain policies to ensure compliance with the Data Protection Act, Human Rights Act, the common law duty of confidence and the Confidentiality NHS Code of Practice;
- The Trust has established and will maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act); and
- The Information Governance legal compliance requirements are linked to the Trust's disciplinary procedures as appropriate.

10.3 Information Security

- The Trust has appointed a Senior Information Risk Officer (SIRO) at Board level;
- The Trust has established and will maintain standards and policies for the

effective and secure use and management of its information assets and resources;

- The Trust has established and will maintain standards and guidance for the effective and secure transfer of information into and out of the Trust;
- The Trust has established and will maintain standards and policies for the disclosure of information;
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements;
- The Trust promotes effective confidentiality and security practice to its staff through policies, procedures and training; and
- The Trust has established and will maintain incident reporting procedures and monitors and investigates all reported instances of actual or potential breaches of confidentiality and security.

10.4 Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance;
- The Trust will undertake or commission annual assessments and audits of its information quality;
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services;
- Wherever possible, information quality should be assured at the point of collection;
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards; and
- The Trust will promote information quality through policies, procedures/ user manuals and training.

10.5 Records Management

- The Trust has established and will maintain policies and procedures for the effective management of records;
- The Trust will undertake or commission annual assessments and audits of its records management;
- Managers are expected to ensure effective records management within their service areas;
- The Trust promotes records management through policies, procedures and training; and
- The Trust uses Records Management: NHS Code of Practice (Part 1 2006; Part 2 revised 2009) as its standard for records management.

10.6 Information Governance Training

- The Trust has established and will maintain the Information Governance Training Programme for the effective delivery of Information Governance training, awareness and education;

- The Trust provides Information Governance induction training directed at all new members of staff;
- The Trust mandates annual mandatory Information Governance training and requires all staff to pass a comprehension assessment;
- The Trust provides general Information Governance awareness on a regular basis through newsletters, articles, team meetings etc; and
- Evaluation of Information Governance training will be undertaken to assess the effectiveness of the training and influence changes to future training.

11 MANAGEMENT OF INFORMATION GOVERNANCE

11.1 The Trust Board is responsible for implementing the Information Governance Policy and supporting management framework and does so via the Information Governance Committee.

11.2 The Trust has appointed a Senior Information Risk Owner (SIRO) at Board level, who chairs the Information Governance Committee and is supported by the Caldicott Guardian, Information Governance & Registration Authority Manager, Information Governance & Registration Authority Officer and Information Governance Committee members. The terms of reference for the Information Governance Committee are given in Appendix 2.

11.3 The Information Governance Committee is supported in delivery of the Information Governance agenda by those sub-committees and working groups that report directly to it. The Information Governance agenda is implemented via the associated policies, procedures and action plans.

11.4 The overall Information Governance Framework is illustrated in Appendix 3. Policies are published and implemented in accordance with the Policy on Policies. The monitoring of compliance with the policies and review of the policies is undertaken in accordance with the monitoring and review statements in each policy.

12 EQUALITY IMPACT ASSESSMENT

12.1 A Stage 1 (Screening) - Equality Impact Assessment has been undertaken and no negative impact on any group was indicated (see Appendix 1).

13 REFERENCES

13.1 References to Standards

- Information Governance Toolkit v.10

13.2 Legislation

- Abortion Regulations 1991 and subsequent amendments
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Data Protection Act 1998
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Health and Social Care Act 2008

- Human Fertilisation and Embryology Act 1990
- Human Rights Act 1998
- Mental Capacity Act 2005
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Re-use of Public Sector Information Regulations 2005

13.3 **Guidance**

- Caldicott Guardian Manual 2010
- Caldicott Report 1997
- Care Quality Commission / Monitor – registration / authorisation and annual assessments
- Care Record Guarantee 2009
- Confidentiality: NHS Code of Practice 2003
- Health Service Circular 1999/012
- Information Security Management: NHS Code of Practice 2007
- NHS Information Governance: Guidance on Legal and Professional Obligations 2007
- NHS Litigation Agency Risk Management Standards
- Records Management: NHS Code of Practice - Part 1 2006, Part 2 2009

14 ARRANGEMENTS FOR MONITORING COMPLIANCE WITH THIS POLICY

Compliance with this policy will be monitored in the following manner (see table below):

Key elements (Minimum Requirements)	**Process for Monitoring (e.g. audit)**	**By Whom (Individual / group /committee)**	**Frequency of monitoring**	**Responsible individual / group / committee (plus timescales(for**		
				Review of Results	**Development of Action Plan**	**Monitoring of action plan and implementation**
Roles and responsibilities	Monitored at appraisal, following review of the individual's knowledge & skills framework (KSF) together with the job description.	Line manager	Annually			
How the organisation provides IG Training. In house training sessions are delivered regularly throughout the year to meet the needs of the Trust	Electronic Staff Record (ESR) is utilised to identify all staff who are non-compliant	IG Team	Monthly	Information Governance Committee	IG Mandatory Training Working Group	Information Governance Committee
Reducing the number of Information Governance breaches	Management of incidents relating to Information Governance	IG Team	Monthly	Information Governance Committee	IG Team	Information Governance Committee
Ensuring best practice across the Trust	Undertaking Confidentiality Audits	IG Team	Monthly	Information Governance Committee	IG Team	Information Governance Committee

APPENDIX 1 EQUALITY IMPACT ASSESSMENT

To be completed and attached to any policy document when submitted to the appropriate committee for ratification

STAGE 1 - SCREENING

Name & Job Title of Assessor: Phil Cottis, Information Governance & RA Manager	**Date of Initial Screening: 01.12.09**
Policy or Function to be assessed: Information Governance Policy	

			Yes/No	Comments
1.	**Does the policy, function, service or project affect one group more or less favourably than another on the basis of:**			
	3.1	Race & Ethnic background	No	This policy is applied equally to all groups
	3.2	Gender including transgender	No	This policy is applied equally to all groups
	3.3	Disability:- This will include consideration in terms of impact to persons with learning disabilities, autism or on individuals who may have a cognitive impairment or lack capacity to make decisions about their care	No	This policy is applied equally to all groups
	3.4	Religion or belief	No	This policy is applied equally to all groups
	3.5	Sexual orientation	No	This policy is applied equally to all groups
	3.6	Age	No	This policy is applied equally to all groups
2.	**Does the public have a perception/concern regarding the potential for discrimination?**		No	This policy is applied equally to all groups

If the answer to any of the questions above is yes, please complete a full Stage 2 Equality Impact Assessment.

Signature of Assessor: Phil Cottis, Information Governance & RA Manager Date: 05.12.12

Signature of Line Manager: Barbara Cummings: Director of Planning & Performance Management Date: 05.12.12

APPENDIX 2 INFORMATION GOVERNANCE COMMITTEE TERMS OF REFERENCE

Information Governance Committee: Terms of Reference

Overall Purpose

The Information Governance Committee is a standing committee accountable to the Trust Board. Its purpose is to support and drive the broader Information Governance agenda and provide the Board with the assurance that effective Information Governance best practice mechanisms are in place within the organisation and to oversee the implementation of those areas of work that sit within the Information Governance framework.

Responsibilities

- To ensure that an appropriate comprehensive Information Governance (IG) framework and systems are in place throughout the organisation in line with national standards
- To undertake an annual baseline assessment and performance update of the IG work areas using the Department of Health IG Toolkit
- To prepare the annual final submission against the IG Toolkit, and to report this to the Board
- To maintain the IG Policy and associated IG framework, and to develop this as required
- To develop and implement an annual action plan for the IG work areas
- To use the action plan as a means of performance managing the IG work throughout the year
- To ensure there are clear lines of authority and accountability for members of staff leading the implementation of the discrete areas of work in the action plan
- To receive regular progress reports from members of staff leading a discrete area of work
- To approve contingency plans where progress has deviated from the plan
- To monitor the organisation's information handling activities to ensure compliance with law and guidance
- To monitor and review untoward occurrences and incidents relating to IG and ensure that effective remedial and preventative action is taken. Serious Incidents (SIs) concerning information risk will be reported to the SIRO, and then reported to the Trust Board.
- To drive the IG training agenda via implementation of the IG Training Programme, ensuring the Trust's approach to information handling is communicated to all staff
- To provide a focal point for the resolution and / or discussion of IG issues

Reporting Committees / Groups

- Health Records Committee
- Corporate Records Committee
- IT IG Working Group
- Data Quality Forum
- Registration Authority Working Group
- Integrated Identity Management Project Board
- IG Mandatory Training Working Group
- IG Toolkit action plan working groups as appropriate

Accountability

- Non-Clinical Governance Committee
- IT Strategic Programme
- Healthcare Governance Committee

Chair / Deputy Chair

- Chair – Senior Information Risk Owner
- Deputy Chair – Caldicott Guardian

Membership

Senior Information Risk Owner – Director of Planning & Performance
Caldicott Guardian
Deputy Director of Performance and Informatics
Company Secretary
Complaints Manager
Head of Communication
Head of ICT
Head of Legal Services
Head of Performance
Health Records Manager
Head of Risk Management
Human Resources & Organisational Development representative
Divisional representative
Clinical representative
Nursing representative
Information Governance & RA Manager
Information Governance & RA Officer
Emergency Planning Officer
HIS Manager
Others – *by invitation depending on the agenda items and current projects*

Deputies should be sent to meetings

Quorum

A quorum shall be 6 members, including the Chair or Deputy Chair.

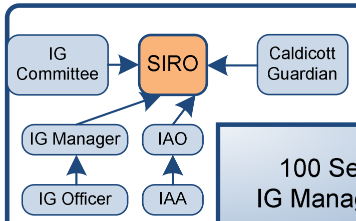
Frequency

Bi-Monthly - additional meetings to be convened if required.

Minutes

Formal minutes will be kept of the proceedings and submitted for approval at the next meeting.

APPENDIX 3 OVERALL INFORMATION GOVERNANCE FRAMEWORK



Overall IG Framework

	100 Series - IG Management	200 Series - Confidentiality/Data Protection Assurance	300 Series - Information Security Assurance	400 Series - Clinical Information Assurance	500 Series - Secondary Use Assurance	600 Series - Corporate Info Assurance
Policies	• IG Policy • Information Risk Policy • Information Lifecycle and Records Management Policy • Corporate Governance Policy	• Data Protection Policy • Access to Health Records Policy and Procedure • Photography and Conventional or Digital Video Records (Clinical) Policy	• Policy & Procedure for the Management of Adverse Events • Information Security Policy • Internet and Email Acceptable Use Policy • Mobile Computing Policy • Access to Trust IT Systems (External Organisations) Policy • Disposal of IT Equipment and Media Policy • RA Operational Policy and Procedure • Data Encryption – Security of Email and Removable Media Policy • Forensic Readiness Policy	• Health Records Management Policy	• Disclosure of Information Policy	• FOI Policy
Related documents	• IG Strategy • IG Action Plan • Information Lifecycle and Records Management Strategy and Implementation Plan • IG Training Programme • IG contract clauses • IG employment contract clauses • 'What is IG?' staff guide	• Confidentiality Code of Conduct • Information Sharing Protocol • Data Exchange Agreement • DPA re-registration	• Safe Haven Procedure • Information Asset Register • IG Checklist for Projects and System Releases • Information Risk Management Assessments • Guide to the Safe Use of Personal Mobile Media • Guide for encrypting CDs • Privacy Impact Assessments (small scale / full scale)			• Protocol for Handling FOI Requests • Creation of Corporate Records Procedure • Inventory of Corporate Records Action Plan
Committees / Working Groups	• IG Committee • IG Mandatory Training Working Group		• RA Working Group • Integrated Identity Management Project Board • Information Technology Working Group		• Data Quality Forum	• Corporate Records Committee • Medical Records Committee

PLAN FOR DISSEMINATION OF PROCEDURAL DOCUMENTS

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Acknowledgement: University Hospitals of Leicester NHS Trust

Title of document:	**Information Governance Policy**		
Date finalised:		**Dissemination lead: Print name and contact details**	**Phil Cottis** **IG & RA Manager** **phil.cottis@qehkl.nhs.uk**
Previous document already being used?	**Yes**		
If yes, in what format and where?	**Electronic format on IG Intranet page & Policies & Procedures: Information Management & Governance**		
Proposed action to retrieve out of date copies of the document:	**Remove outdated policy from Trust Intranet**		
To be disseminated to:	**How will it be disseminated, who will do it and when?**	**Format**	**Comments:**
All staff	**IG Intranet page & Policies & Procedures: Information Governance**	**Electronic**	**Trust Staff advised through IG newsletter and email to Management Forum**

Dissemination Record - to be used once document is approved

Date put on register / library of procedural documents:		**Date due to be reviewed:**	

Disseminated to: (either directly or via meetings, etc.)	**Format (i.e. paper or electronic)**	**Date Disseminated:**	**No. of Copies Sent:**	**Contact Details / Comments:**

CHECKLIST FOR THE REVIEW AND APPROVAL OF PROCEDURAL DOCUMENTS
To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	Information Governance Policy	
		Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Is the method described in brief?	Yes	
	Are individuals / stakeholders / users involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are local/organisational supporting documents referenced?	Yes	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	Does the document identify which committee will ratify it?	Yes	
	If appropriate, have the joint Human Resources/staff side committee (or equivalent) approved the document?	NA	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it	Yes	

	Title of document being reviewed:	Information Governance Policy	
		Yes/No/ Unsure	Comments
	will be held?		
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process for Monitoring Compliance**		
	Are there measurable standards or KPIs to support monitoring compliance of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so, is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	Yes	

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Phil Cottis	**Date**	11th January 2013
Signature			
Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Barbara Cummings	**Date**	13th February 2013
Signature			

Acknowledgement: Cambridgeshire and Peterborough Mental Health Partnership NHS Trust