Camden and Islington NHS
NHS Foundation Trust

INFORMATION GOVERNANCE/SECURITY MANAGEMENT FRAMEWORK AUGUST 2014

This Policy supersedes all previous policies for The Information Governance Framework

Version 3.0

Your partner in care & improvement

Framework Title	Information Governance/Security Management Framework
Relevant to	All Staff
Date published	September 2011
Implementation date	September 2011
Date last reviewed	August 2014
Next review date	August 2015
Policy lead	Information Governance Manager
Contact details	Email: Information.governance@candi.nhs.uk Telephone: 020 3317 3115
Accountable Director	Claire Johnston, Director of Nursing & People
Approved by (Group):	Information Governance Steering Group
Approved by (Committee):	Information Governance Steering Group

Document history

Date	Version	Amendments
Sept 2011	1.0	
Aug 2013	2.0	
Sept 2014	3.0	Job titles, structure, reporting, Policy matrix, Guidance and Training, Incident Management

Membership of the Policy development/ review team	Information Governance Steering Group
Consultation	Information Governance Steering Group

DO NOT AMEND THIS DOCUMENT

Further copies of this document can be found on the Foundation Trust Intranet.

Contents

1. Introduction

The Information Governance Framework brings together related initiatives concerned with improving the security, processing, quality and handling of information. It incorporates the Data Protection Act 1998, the Freedom of Information Act 2000, the Human Rights Act 1998 and the common law duty of confidence. It also incorporates the NHS Code of Confidentiality; Information Security Assurance (compliance with ISO 27001 and equivalent), Information Quality Assurance and Records Management and underpins the NHS Care Record Guarantee.

2. Aims and Objectives

The purpose of this document is to provide a robust management framework to ensure that delivery of internal Information Governance/Security is achieved across the Trust in line with national guidelines

3. Scope of the Framework

The Information Governance/Security Management Framework is the control assurance framework which is formed by those elements of law and policy from which applicable Information Governance/Security standards are derived.

4. Information Governance/Security Roles & Responsibilities

IG Function	Job Title
Chief Executive	Wendy Wallace
Lead Director	Claire Johnson, Director of Nursing and People
Senior Information Risk Owner (SIRO)	Claire Johnston, Director of Nursing and People
Caldicott Guardian **Deputy Caldicott**	Dr. Vincent Kirchner, Medical Director Jeff Halperin, Clinical Director
ICT Lead, Information Governance/Security	David Jackal, Associate Director of ICT
Information Governance/ Security	Umar Sabat, Information Governance Manager

5. Resources

Head of Quality Assurance and Regulation will hold the budget for internal Information Governance/Security and is responsible for highlighting any resourcing issues and improvements required for 2014/2015.

6. Current Information Governance/Security Related Policies

Type	Policy/Guidance/Procedure	Current Version
Policy COR 06	Access to Health Records Policy	V3.0 August 2014
Policy COR 32	Data Encryption Policy	V2.0 September 2013
Policy COR18	Data Protection Policy	V3.0 August 2014
Policy COR 20	E-mail Policy	V3.0 September 2013
Policy COR 31	Freedom of Information Policy	V3.0 August 2014
Policy COR 38	ICT Disposal and Destruction Policy for Equipment and Media	V2.0 September 2013
Policy COR 21	Information Security Policy	V1.0 October 2013
Policy COR 23	Internet Connection and Acceptable Use Policy	V2.0 September 2013
Policy COR 2	Corporate Records Management Policy	V3.0 August 2014
Policy COR 22	Information Governance Policy	V3.0 August 2014
POLICY RM03	Incident Reporting Policy	V2.0 August 2011
Policy COR 39	Telecommunications Policy	V2.0 September 2013
Policy COR 40	Mobile Computing Policy	V2.0 September 2013
Policy COR 41	Remote Access Policy	V2.0 September 2013

All Policies are reviewed and updated where applicable on a regular basis and ratified by the Trust's Information Governance Steering Group. The Policies have been placed on the Trust's Intranet for all staff to be able to access easily.

7. Guidance/Training and Awareness

- Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedure. This is achieved by:

- All staff are currently briefed on Information Governance/Security requirements as part of their induction.

- Training Sessions for specific departments/teams.

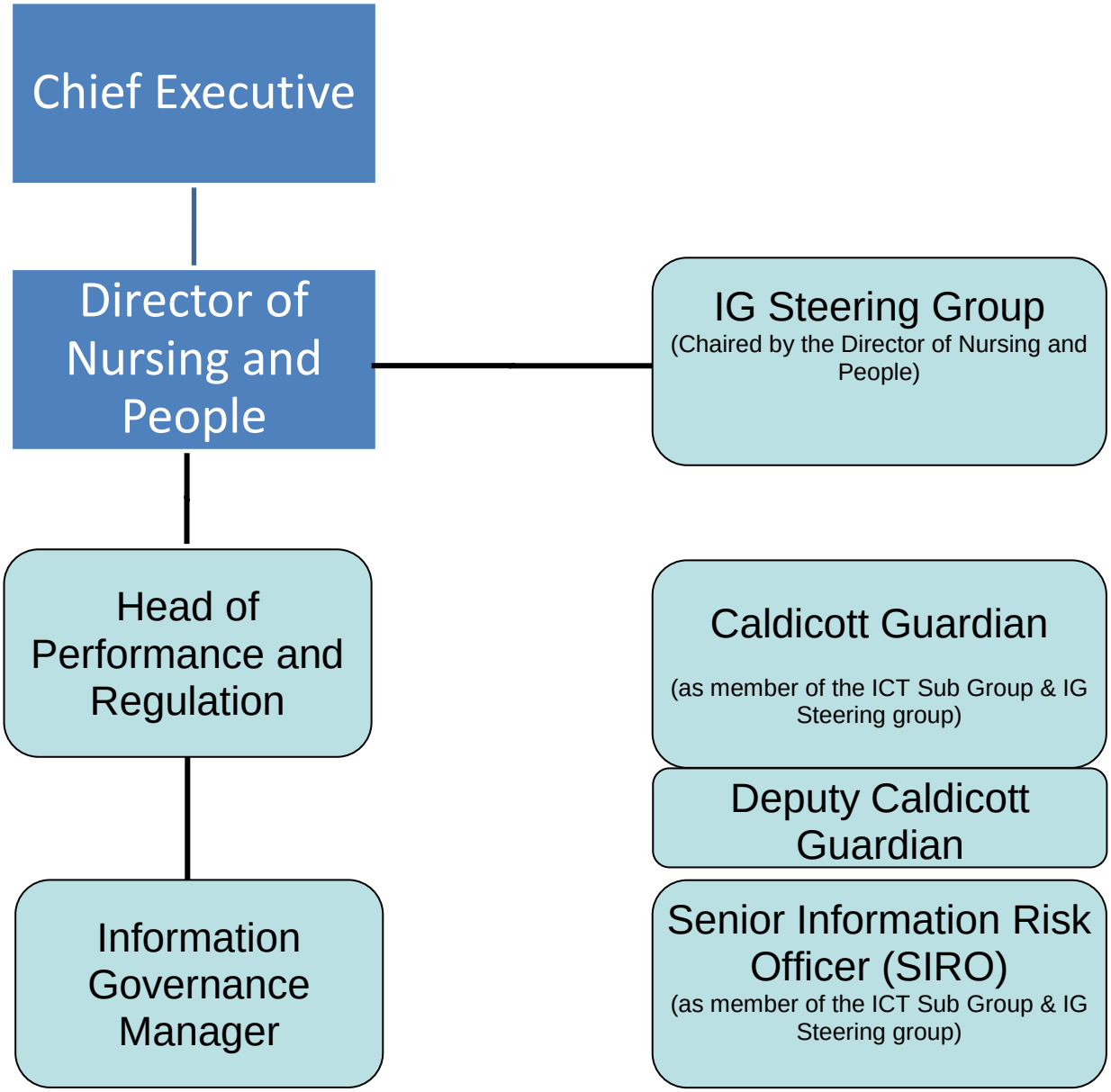
- Staff requirement to complete the Information Governance/Security training tool on an annual basis.

- The Information Governance/Security Department looks to raise awareness and governance/security standards throughout the Trust. The Department is using the Intranet to disseminate all types of IG/IS information, using the staff bulletin to ensure that all staff are aware of their responsibilities.

8. Incident Management

The Trust has Incident Management procedures in place. It raises incidents through this route via Datix. Impact of the new reporting through the IG Toolkit has been reviewed and is done in conjunction with the Trust process.

9. Structure of Information Governance/Security



10. Information Governance Internal Reporting

The Information Governance/Security Department reports every two months to the IG steering group. The following are reported as standard items:

- Information Governance Update (incorporating FOI & Data Protection issues, incidents)
- Information Security Update
- IG Toolkit – Specific Update on progress
- IG training
- Policies for approval where applicable

11. Review of the Framework

This Framework should be reviewed every year from implementation date as a minimum. This Framework may also be reviewed and amended at any time if it is considered that amendments are required to ensure the Framework is up to date and accurate for the Trust.

Any amendments to this Policy will need to be approved by the Information Governance Steering group.

Appendix 1 - Equality Impact Assessment Tool

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

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**	No	
	Race	No	
	Ethnic origins (including gypsies and travellers)	No	
	Nationality	No	
	Gender	No	
	Culture	No	
	Religion or belief	No	
	Sexual orientation including lesbian, gay and bisexual people	No	
	Age	No	
	Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

If you have identified a potential discriminatory impact of this procedural document, please refer it to the author together with any suggestions as to the action required to avoid/reduce this impact.