Northampton General Hospital NHS
NHS Trust

This document is uncontrolled once printed.

Please refer to the Trusts Intranet site (Procedural Documents) for the most up to date version

INFORMATION SECURITY

NGH-PO-011

Ratified By:	Procedural Documents Group
Date Ratified:	April 2016
Version No:	3
Supercedes Document No:	2
Previous versions ratified by (group & date):	March 2014
Date(s) Reviewed:	March 2016
Next Review Date:	March 2019
Responsibility for Review:	Information Governance Manager
Contributors:	IG Steering Group

POLICY

CONTENTS

Version Control Summary

Version	Date	Author	Status	Comment
1.3	28 November 2008	Hospital Management Group	Final	New document
1.3.1	4 June 2013	Louise Chatwyn – Information Governance Manager	Draft	Policy due for review to reflect changes in the use of IT systems
1.3.2	15 January 2014	Kehinde Okesola – Information Governance Manager	Draft	Policy review and transfer to the new Trust policy template
1.4	5 February 2014	Kehinde Okesola – Information Governance Manager	Draft	Implementation of minor comments from the policy consultation process
2	March 2014	Kehinde Okesola – Information Governance Manager	Ratified	
3	March 2016	Kehinde Okesola – Information Governance Manager	Draft	Policy review due to changes in the IG reporting structure.

SUMMARY

The Information Security Policy refers to standards, policies and procedures as well as legal guidance which are used to develop and support systems in keeping information secure and confidential. Ensuring the 3 main information security principles are met. These principles are:

- Confidentiality
- Integrity
- Availability

1. INTRODUCTION

Information held in electronic and manual information systems within the Trust represents one of its most valuable assets. It is therefore essential that all computers, networks and information contained within them are protected against the many threats which may compromise the data, patient or staff privacy and/or the overall service provision.

Information is one of the Trust’s key assets. It is essential that patient and NHS information is kept confidential and secure.

In support of this, every member of staff has a personal responsibility to maintain the security and confidentiality of Trust-held information and to always treat this information in a professional and ethical manner. This policy is intended to inform all staff of their responsibilities and to help them meet these requirements.

The Trust is committed to achieving the highest possible standard of security of information that it holds about patients, staff and its business, whether that information is contained in electronic formats or manually produced records. It will further ensure that staff adhere to ethical standards of confidentiality in order to sustain public confidence in the Trust's provision of care.

Failure to act within these guidelines will render staff liable to the Trust’s disciplinary process. In cases of serious misconduct involving personal data, the Trust will consider prosecution under the appropriate legislation.

This top-level information security policy is a key component of the Trust’s overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

2. PURPOSE

The policy aims to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or managed by the Trust by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies. Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

3. SCOPE

This policy applies to:

- All information, information systems, networks, application systems and users;
- All sites used by the Trust;
- All those having access to information employed by the Trust, including temporary staff; contractors and agency staff;
- All those engaged in duties for the Trust under a Letter of Authority, Honorary Contract or Work Experience programme;
- Volunteers and all Third parties such as contractors, researchers, students or visitors.

4. COMPLIANCE STATEMENTS

Equality & Diversity

This policy has been designed to support the Trust's effort to promote Equality, Diversity and Human Rights in the work place and has been analysed for any adverse or negative impact using the Trust's Equality Analysis toolkit as required by the Trust's Equality and Human Rights Strategy. It is considered to be compliant with equality legislation and to uphold the implementation of Equality, Diversity and Human Rights in practice.

NHS Constitution

The contents of this document incorporates the NHS Constitution and sets out the rights, to which, where applicable, patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with the responsibilities which, where applicable, public, patients and staff owe to one another. The foundation of this document is based on the Principals and Values of the NHS along with the Vision and Values of Northampton General Hospital NHS Trust.

5. DEFINITIONS

ICT	Information and communications technology
IM&T	Information Management and Technology
IG SIRI	Information Governance Serious Incident Requiring Investigation. Such incidents must be reported to the Information Commissioners Office (ICO)
Information Asset Owners (IAOs)	The Information Asset Owner (IAO) is a mandated role, and the individual appointed is responsible for ensuring that specific information assets are handled and managed appropriately.

6. ROLES & RESPONSIBILITIES

ROLE	RESPONSIBILITY
Chief Executive and the Trust Board	Chief Executive and Trust Board have ultimate accountability for actions and inactions in relation to this policy. On behalf of the Chief Executive, the Senior Information Risk Owner (SIRO), with support from the Information Security Manager and the Information Governance Manager will be responsible for implementing, monitoring, documenting and communicating information security and management requirements throughout the Trust. The Information Security Manager and the Information Governance Manager will act as a focal point for resolution to discuss information risk issues that may affect the Trust and report any risk to the SIRO.
Senior Information Risk Owner (SIRO)	The Director of Corporate Development Governance and Assurance is the SIRO for the Trust. The SIRO will take ownership of Trust's information risk and security management, act as advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of the Statement on Internal Control in regard to information risk.
Caldicott Guardian	The Medical Director is the Caldicott Guardian at the Trust. The Caldicott Guardian has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with safe haven guidelines and the Caldicott principles
Information Governance Manager	The Information Governance Manager is responsible for the implementation and enforcement of the Information Security Policy.

	• Ensuring that the Trust complies with the Data Protection Act 1998 and that • Information Governance standards are effectively managed and implemented throughout the Trust.
Information Security Manager	The Information Security Manager is responsible for ensuring the day to day security of the Trust's electronic network and equipment, In this Trust, the Information Security Manager is the IT Service Delivery Manager.
Information Asset Owners (IAOs)	Information Asset Owners (IAO) will act as nominated owner of one or more information assets of the Trust. Their responsibilities will also include: • Identify Information Asset Administrators to assist them with their duties, where this is appropriate and necessary. • Document, understand and monitor what information assets are held, and for what purpose, how information is created, amended or added to, who has access to the information and why. • Identify information necessary in order to respond to incidents or recover from a disaster affecting the information asset. • Take ownership via input to the Trust's Information Asset Register of their local asset control, risk assessment and management processes for the information assets they own, including the identification, review and prioritisation of perceived risk and oversight of actions agreed to mitigate those risks. • Provide support to the SIRO to maintain awareness of risks to all information assets, for the purpose overall risk reporting requirements and procedures. • Ensure that relevant staff are aware of and comply with expected Information Governance working practices for the effective use of owned information assets
Line Managers	Line Managers will take responsibility for ensuring that their permanent, temporary and contractor staff are aware of: • Information security policies applicable in their work areas. • Personal responsibilities for information security. • How to access advice on information security matters. • Ensure that their staff have had suitable security training in accordance with the mandatory IG training. • Line managers are individually responsible for the security of their physical environments where information is processed or stored.
All Trust Employees	Have a responsibility to: • Support the Trust to achieve its Vision and Values • Follow duties and expectations of staff as detailed in the NHS Constitution – Staff Responsibilities

	Each member of staff shall be responsible for the operational security of the information systems they use; e.g. using (and not sharing) passwords, logging on and off and applying appropriate physical security. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard. The information security undertaking must be signed by all staff before commencing their employment (Information security form– appendix 1)

7. SUBSTANTIVE CONTENT

7.1. Job Descriptions and Contracts of Employment

Information security expectations of staff shall be included within appropriate job descriptions.

All contracts of employment shall contain a data protection, confidentiality and standards of conduct clause.

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Information security expectations of staff shall be included within appropriate job descriptions.

7.2. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named information Asset Owner and Administrator who will be responsible for the information security of that asset.

7.3. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

User Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

7.4. Computer Access

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities. Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the IT Sub-Committee.

7.5. Security

Physical Security

Physical environment should be recognised as providing a layer of protection to data and information. This is achieved by the following means:

- Controlling access to sites, buildings and offices.
- Ensuring desks and work areas are clear at the end of each day.
- Use of locked cabinets within offices to restrict access to information.
- Checking that visitors to sites are authorised to be there.
- Ensuring that when information is carried off site, it is held securely in a locked case.
- Always wearing your ID badge when on site.

Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

7.6. Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the Trust’s risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

7.7. Information security Breaches and Near-Misses

All information security breaches, Serious Untoward Incidents, near-misses, and suspected weaknesses via the Trusts incident reporting system (Datix). Information security breaches are also to be reported to the Information Governance Manager (extension 3881). All information security breaches shall be investigated to establish their cause and impacts with a view to avoiding similar events. IG SIRIs will be managed in line with the Trust’s IG Incident Management Protocol.

7.8. Classification of Sensitive Information

The Trust will implement appropriate information classifications controls, necessary to secure NHS information assets. New Government Security Classifications (published April 2013) have been implemented to assist in deciding how to share and protect information.

The classification OFFICIAL-SENSITIVE: PERSONAL (Formally NHS Confidential) – shall be used for patients' clinical records, patient identifiable clinical information passing between NHS staff and between NHS staff and staff of other appropriate agencies. In order to safeguard confidentiality, the term "NHS Confidential" shall not be used on correspondence to a patient in accordance with the Confidentiality: NHS Code of Practice. Documents so marked shall be held securely at all times in a locked room to which only authorised persons have access. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed packaging or locked containers. Documents marked NHS Confidential not in a safe store or in transport should be kept out of sight of visitors or others not authorised to view them.

The classification OFFICIAL-SENSITIVE: COMMERCIAL (formally NHS Restricted) - shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- Adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness of the organisation;
- Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- Prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- Breach statutory restrictions on disclosure of information;
- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

OFFICIAL-SENSITIVE: COMMERCIAL documents should also be stored in lockable cabinets

7.9. Information Sharing for Safeguarding Issues

The Trust has information sharing protocols with both the police, the Local children's Safeguarding Board, the Multiagency Risk Assessment Conference (Domestic Abuse) and the Child Exploitation Forum (please refer to the Safeguarding Children's policy [NGH-PO-243]) for the purpose of safeguarding children. Information can be shared with these organisations when there are legitimate concerns. If in doubt, check with the safeguarding team (ext. 3218)

7.10. Protection from Malicious Software

The Trust will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff are expected to co-operate fully with this policy. Users shall not install software on the Trust's property without permission from the Head of ICT. Users breaching this requirement may be subject to disciplinary action.

7.11. User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Deputy Director of IT before they may be used on Trust systems. Such media must also be fully virus checked before being used on the Trust's equipment.

Staff must ensure that only Trust approved USB/memory sticks are used for work purposes. The use of an unencrypted portable device such as a memory stick to transfer personal data is prohibited. Users breaching this requirement may be subject to disciplinary action.

7.12. Appropriate Conduct by Staff

Every member of staff has a responsibility to maintain the security and confidentiality of Trust-held information and to treat such information in a professional and ethical manner. Before using electronic mail (e-mail) and/or the Internet at work, staff should read the relevant policies as outlined in section 10 and associated documentation note that:

- These services are provided primarily for Trust business use and for appropriate professional use and career development;
- Limited personal use is acceptable outside normal working time;
- Other uses are not permitted;
- E-mail use and Internet access is monitored by the Trust.

The Trust's Electronic Mail and Internet Policy includes restrictions and prohibitions regarding email content, Internet site access and the use of Social Media. The following extract is intended to remind staff of Trust restrictions in place. Staff should note that these restrictions do not form a complete list of Trust email and Internet restrictions included in the Trust's Electronic Mail and Internet Policy.

- Emails should not contain messages that are illegal, abusive, obscene or defamatory
- Emails should not contain images that are pornographic or otherwise indecent
- Emails should not contain material that insults or harasses others
- Emails should not make any improper or defamatory reference as per the protected characteristics as detailed in the Equality Act 2010.
- Emails should not be used to participate in electronic chain letters

Internet access MUST NOT be used:

- To access sites that contain illegal, abusive, obscene or defamatory material
- To access sites that contain images that are pornographic or otherwise indecent
- To participate in chat rooms & social networking sites (except official Discussion Boards)
- To download personal files (music, movie etc.) to any part of the Trust's infrastructure. Staff are also reminded that personal mobile telephones, PDAs and

other devices with digital cameras or photographic capability must not be used for non-approved Trust business purposes to record images at work that:

- Contain confidential or patient-identifiable information;
- Include patients or their friends and family; unless with their express permission;
- Invade any individual's privacy or dignity.

7.13. Mobile Devices with Cameras, Videos and Audio Recording Functions

Most mobile telephones and electronic devices (tablet devices, PDA devices etc.) have the facility to record photographic/video images or audio recording. The use of these devices in patient areas by patients, staff, visitor or contractor is likely to result in inappropriate photographs being taken or taken without the correct consents. This would be in breach of: patient privacy & dignity, patient confidentiality and, in the case of children, the Trust's obligation to safeguard and promote the welfare of children.

Personal mobile devices must not be used to take pictures of patients, store or send confidential patient data. This applies to audio, video, still photograph or any other form of electronic data. Users breaching this requirement may be subject to disciplinary action.

7.14 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis by the Information Asset Owner or the IG Manager.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.
- Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

7.15 Accreditation of Information Systems

The Trust will ensure that all new information systems, applications and networks include a security plan and are approved by the Deputy Director of IT before they commence operation.

7.16 System Change Control

Changes to information systems, applications or networks will be reviewed and approved by the Deputy Director of IT.

7.17 Intellectual Property Rights

The Trust will ensure that all information products are properly licensed and approved by the Deputy Director of IT. Users shall not install software on the Trust's property without permission from the Deputy Director of IT. Users breaching this requirement may be subject to disciplinary action.

7.18 Business Continuity and Disaster Recovery Plans

The Trust will ensure that business impact assessment, business continuity and disaster recovery plans are produced for all critical information, applications, systems, departments and networks.

7.19 Reporting

The Information Governance Manager and Information Security Manager will keep the Information Governance Group informed of the information security status of the Trust by means of regular reports and presentations.

7.20 Further Information

Further information and advice on this policy can be obtained from the Information Governance Manager Ext 3881.

8. IMPLEMENTATION & TRAINING

Training and guidance on the Information Security Policy is available and managers must ensure that their staff are fully aware of its implications. The principles of information security require that all reasonable care be taken to prevent the inappropriate access, modification or manipulation of data.

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

9. MONITORING & REVIEW

Minimum policy requirement to be monitored	Process for monitoring	Responsible individual/ group/ committee	Frequency of monitoring	Responsible individual/ group/ committee for review of results	Responsible individual/ group/ committee for development of action plan	Responsible individual/ group/ committee for monitoring of action plan
Incident reports	Adhoc reports through incidents	Information Governance Group	Annually and adhoc reviews (where serious IG incidents have occurred)	This policy shall be subject to audit by Internal Auditors	The Information Governance Manager	The action plan will be reviewed by the IG group with a report to the Assurance, Risk and Compliance (ARC) Group

10. REFERENCES & ASSOCIATED DOCUMENTATION

British Standards Institute (2014) *BS ISO/IEC 27000:2014. Information technology. Security techniques. Information security management systems. Overview and vocabulary*. Milton Keynes: BSI

British Standards Institute (2013) *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements*. Milton Keynes: BSI

Cabinet Office (2013) *Government security classifications April 2014.* [online]. London: TSO. Available from: https://www.gov.uk/government/publications/government-security-classifications [Accessed 22nd March 2016]

Data Protection Act 1998 (c.29) [online] London, HMSO. Available from: http://www.legislation.gov.uk/ukpga/1998/29 [Accessed 24 February 2016]

Department of Health (2013). *NHS Constitution: the NHS belongs to us all.* [online]. London. Department of Health. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/480482/NHS_Constitution_WEB.pdf [Accessed 22nd March 2016]

Department of Health (2007) *Information Security Management: NHS Code of Practice*. London: DH

Department of Health (2007) *Information security management: NHS code of practice.* [online]

London: DH. Available from: http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf [Accessed 22nd March 2016]

Department of Health (2003) *Confidentiality: NHS code of practice*. [online]. London: DH. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf [Accessed 24 February 2016]

Department of Health (n.d) *Information Governance Toolkit: Homepage.* [online]. Available from: https://www.igt.hscic.gov.uk/ [Accessed 22nd March 2016]

Department of Health, Social Services and Public Safety (no date) *The common law duty of confidentiality*. [online]. Available from: https://www.dhsspsni.gov.uk/articles/common-law-duty-confidentiality [Accessed 22nd March 2016].

Equality Act 2010 (ch.15). [online]. London: HMSO. Available from: http://www.legislation.gov.uk/ukpga/2010/15/contents [Accessed 24 February 2016]

Freedom of Information Act 2000 (c.36) [online] London. HMSO. Available from: http://www.legislation.gov.uk/ukpga/2000/36/contents [Accessed 24 February 2016]

Government Equalities Office (2013) *Equality Act 2010: guidance*. [online]. London: Available from: https://www.gov.uk/equality-act-2010-guidance [Accessed 15 January 2014]

Health and Safety at Work etc. Act 1974. (c.37). [online]. London: HMSO. Available from: http://www.legislation.gov.uk/ukpga/1974/37/contents [Accessed 22nd March 2016]

Human Rights Act 1989. (c.42). [online]. London: HMSO. Available from: http://www.legislation.gov.uk/ukpga/1998/42/contents [Accessed 22nd March 2016]

Northampton General Hospital NHS Trust (2016) *Disciplinary Policy*. NGH-PO-028. Northampton: NGHT

Northampton General Hospital NHS Trust (2016) *Freedom of Information Act 2000: policy and procedure*. NGH-PO-096. Northampton: NGHT

Northampton General Hospital NHS Trust (2016) *Transmission of confidential information (Safe Haven).* NGH-PO-066. Northampton: NGHT

Northampton General Hospital NHS Trust (2016*) Information incident management procedures.* NGH-PT-575. Northampton: NGHT

Northampton General Hospital NHS Trust (2016) *Use of mobile phones and mobile communications*. NGH-PO-009. Northampton: NGHT

Northampton General Hospital NHS Trust (2015) *Electronic mail and internet*. NGH-PO-10-02. Northampton: NGHT

Northampton General Hospital NHS Trust (2015) *Data protection and confidentiality policy*. NGH-PO-334. Northampton: NGHT

Northampton General Hospital NHS Trust (2013) *Equality and Human Rights Strategy 2013-2016*. Northampton: NGHT

Northampton General Hospital NHS Trust (2013) *Photography and video recording of patients*. NGH-PO-068. Northampton: NGHT

Northampton General Hospital NHS Trust (2012) *Safeguarding children*. NGH-PO-243. Northampton: NGHT

Regulations of Investigatory Powers Act 2000 (c.23) [online] London, HMSO. Available from http://www.legislation.gov.uk/ukpga/2000/23/contents [Accessed 24 February 2016]

APPENDICES

Appendix 1: INFORMATION SECURITY POLICY UNDERTAKING

UNDERTAKING TO MAINTAIN INFORMATION SECURITY & CONFIDENTIALITY

I acknowledge receipt of the Trust's Information Security Policy, and undertake to treat any information that I may acquire in the course of my work, whether it is about patients or any other sensitive matter, with the strictest confidence, and not to discuss it with any other person unless they are directly concerned in the matter.

I shall not read medical case notes unless this is part of my duties, or access any computer system for which I have not been issued a password.

I understand that it is a disciplinary offence to install private software in any computer owned by the Trust.

I accept that the giving of this undertaking forms part of my Contract of Employment, and also that many of the obligations are statutory.

Name:..

Position:...

Signature:..

Date:...

Signature of Witness:..

Status of Witness:..

FORM 1a- **RATIFICATION FORM - FOR COMPLETION BY DOCUMENT LEAD**
Note: Delegated ratification groups may use alternative ratification documents approved by the procedural document groups.

DOCUMENT DETAILS	
Document Name:	Information Security
Is the document new?	Yes/[✓ No]
If yes a new number will be allocated by Governance	New Number
If No - quote old Document Reference Number	NGH-PO-011
This Version Number:	**Version: 3**
Date originally ratified:	May 2014
Date reviewed:	March 2016
Date of next review: a 3 year date will be given unless you specify different	**Date:** **Highlight: (1 year) (2 year) [✓ (3 year)]**
If a Policy has the document been Equality & Diversity Impact Assessed? (please attach the electronic copy)	Yes / [✓ No]
DETAILS OF NOMINATED LEAD	
Full Name:	Kehinde Okesola
Job Title:	Information Governance Manager
Directorate:	Governance
Email Address:	Kehinde.Okesola @ngh.nhs.uk
Ext No:	3881
DOCUMENT IDENTIFICATION	
Keywords: **please give up to 10 –** to assist a search on intranet	Information , security, breaches, data protection, mobile devices, ICO

GROUPS WHO THIS DOCUMENT WILL AFFECT?
(please highlight the Directorates below who will need to take note of this updated / new Document)

Anaesthetics & Critical Care	General Medicine & Emergency Care	Medical Physics
Child Health	Gynaecology	Nursing & Patient Services
Corporate Affairs	Haematology & Oncology	Obstetrics
Diagnostics	Head & Neck	Ophthalmology
Estates & Facilities	Human Resources	Planning & Development
Finance	Infection Control	Trauma & Orthopaedics
General Surgery	Information Governance	[✓ Trust Wide]

TO BE DISSEMINATED TO: NB – **if Trust wide document it should be electronically disseminated to Head Nurses/ Dm's and CD's .List below all additional ways you as document lead intend to implement this policy such as; as presentations at groups, forums, meetings, workshops, The Point, Insight, newsletters, training etc below:**

Where	When	Who
Mandatory Training and Induction	Twice monthly induction	All new staff
ROK sessions, training refreshers	As per advertised training schedule or as and when arranged departmentally	All staff groups

FORM 2 - RATIFICATION FORM to be completed by the document lead

Please Note: Document will not be uploaded onto the intranet without completion of this form

CONSULTATION PROCESS

NB: You MUST request and record a response from those you consult, even if their response requires no changes. Consider Relevant staff groups that the document affects/ will be used by, Directorate Managers, Head of Department ,CDs, Head Nurses , NGH library regarding References made, Staff Side (Unions), HR Others please specify

Name, Committee or Group Consulted	Date Policy Sent for Consultation	Amendments requested?	Amendments Made - Comments
Caroline Corkerry	25 February 2016	Inclusion of memory sticks	Included
		Query on a reporting of IG incidents	This has been clarified within the policy. The Trust is mandated to follow the national IG serious incident reporting guidance by HSCIC hence the Trust having a separate incident management protocol for serious IG incidents
Andrea Chown	25 February 2016	None requested	N/A
Michael P De-Manuel Maxillofacial Unit	25 February 2016	Inclusion of mobile phone usage	Included

Existing document only - FOR COMPLETION BY DOCUMENT LEAD

Have there been any significant changes to this document? *if no you do not need to complete a consultation process*		[✓ YES] / NO
Sections Amended:	YES / NO	**Specific area amended within this section**
Re-formatted into current Trust format	[✓ YES] / NO	
Summary/ Introduction/Purpose	YES / NO	
Scope	YES / NO	
Definitions	YES / NO	
Roles and responsibilities	YES / NO	
Substantive content	[✓ YES] / NO	**7.11 and 7.13**
Monitoring	YES / NO	
Refs & Assoc Docs	YES / NO	
Appendices	YES / NO	

FORM 3- RATIFICATION FORM (FOR PROCEDURAL DOCUMENTS GROUP USE ONLY)
Read in conjunction with FORM 2

Document Name:	**Information Security**	**Document No:**	**NGH-PO-011**
Overall Comments from PDG			

	YES / NO / NA	**Recommendations**	**Recommendations completed**
Consultation Do you feel that a reasonable attempt has been made to ensure relevant expertise has been used?	**[✓ YES] / NO / NA**		
Title -Is the title clear and unambiguous?	**[✓ YES] / NO / NA**		
Is it clear whether the document is a strategy, policy, protocol, guideline or standard?	**[✓ YES] / NO / NA**		
Summary Is it brief and to the point?	**[✓ YES] / NO / NA**		
Introduction Is it brief and to the point?	**[✓ YES] / NO / NA**		
Purpose Is the purpose for the development of the document clearly stated?	**[✓ YES] / NO / NA**		
Scope -Is the target audience clear and unambiguous?	**[✓ YES] / NO / NA**		
Compliance statements – Is it the latest version?	**[✓ YES] / NO / NA**	Equality & Diversity section to be updated	Completed
Definitions –is it clear what definitions have been used in the	**[✓ YES] / NO / NA**		
Roles & Responsibilities Do the individuals listed understand about their role in managing and implementing the policy?	**[✓ YES] / NO / NA**		
Substantive Content is the Information presented clear/concise and sufficient?	**YES / [✓ NO] / NA**	7.1 to be reworded Appendix 1 Needs referring to. 7.8 To update NHS Confidential comments	Completed Completed Completed
Implementation & Training – is it clear how this will procedural document will be implemented and what training is required?	**[✓ YES] / NO / NA**		
Monitoring & Review (policy only) -Are you satisfied that the information given will in fact monitor compliance with the policy?	**[✓ YES] / NO / NA**		
References & Associated Documentation / **Appendices**- are these up to date and in Harvard Format? Does the information provide provide a clear evidence base?	**[✓ YES] / NO / NA**	References updated by library	Completed
Are the keywords relevant	**[✓ YES] / NO / NA**		

Name of Ratification Group: Procedural Documents Group	**Ratified Yes/No:** **Ratified subject to chair approval**	**Date of Meeting:** **21/04/2016**
