TRANSMISSION OF CONFIDENTIAL INFORMATION (Safe Haven)

NGH-PO-066

Ratified By:	Chair Approval
Date Ratified:	July 2016
Version No:	4
Supercedes Document No:	3.7.2
Previous versions ratified by (group & date):	Procedural Documents Group
Date(s) Reviewed:	April 2014, June 2016
Next Review Date:	July 2019
Responsibility for Review:	Information Governance Manager
Contributors:	Information Governance Manager

POLICY

CONTENTS

POLICY

Version Control Summary

Version	Date	Author	Status	Comment
1.0	January 1994		Original Final	
2.0	January 2009		Final	
3.0	February 2012	Ian Garratt - Data Protection and Confidentiality Manager	Draft	
3.7.1	February 2012	Ian Garratt - Data Protection and Confidentiality Manager	Final	Ratified by PDG with Minor Amendments
3.8	February 2014	Kehinde Okesola – Information Governance Manager	Ratified	Reviewed with no amendments. Transferred to new Trust policy Template
4.0	May 2016	Kehinde Okesola – Information Governance Manager	Draft	

SUMMARY

Information is an invaluable asset to the Trust and the NHS. Information transfers and sharing information is crucial in order to maximise its potential and provide the most effective patient care.

Confidentiality is part of the duty of care to a patient and owed to all employees of the Trust. The transmission of patient or staff identifiable information must therefore be undertaken in a manner which preserves their confidentiality; this is achieved by using safe haven procedures for such transfers.

Safe Haven procedures are arrangements that have been put in place to ensure confidential information can be communicated safely and securely.

This policy details the Trust's Safe-Haven arrangements in place to ensure that transfer of all person-identifiable information into and from the organisation is undertaken according to the Caldicott Principles, Data Protection Act and other legislative requirements and guidance, irrespective of whether or not the purpose is directly related to the provision of care.

By following the guidelines in this policy, the Trust can ensure that information is processed legally whilst also providing access when required in a format appropriate for the end user.

1. INTRODUCTION

Information is constantly transferred between individuals, departments and organisations. It is essential that the transfer of personal and sensitive information is done so securely and confidentially.

The Trust has a legal obligation to protect the security of its information assets and the duty of care to patients extends to maintaining confidentiality. This policy details the standard approach to be followed when sending information in a manner in which staff and patients can be confident that the transfer has occurred securely, professionally and in accordance with the Data Protection Act 1998 and the Caldicott Principles.

2. PURPOSE

The purpose of this policy is to ensure that the confidentiality of information is maintained within all areas of the Trust and with all of the Trust's information assets. Where there is a need to transfer, transport, distribute or access information, staff must ensure that confidentiality is not breached.

There is always a risk when transferring information. This policy is designed to reduce these risks and assist in helping the Trust meet its statutory obligations in data processing.

3. SCOPE

This policy applies to:

a) All NGH information assets, whether electronic, physical or other

b) All equipment that is, or can be, used to transmit information including, but not limited to, telephones, faxes and email accounts and portable storage devices such as USB sticks.

c) All personal equipment which is used for anything related to NGH or its business, patients, or staff

d) All sites used by the Trust

e) All persons who use or have access to any of the above mentioned in 3 a), 3 b), 3 c) or 3 d)

4. COMPLIANCE STATEMENTS

Equality & Diversity

This document has been designed to support the Trust's effort to promote Equality, Diversity and Human Rights in the work place in line with the Trust's Equality and Human Rights Strategy. It has also been analysed to ensure that as part of the Public Sector Equality Duty the Trust has demonstrated that it has given 'due regard' to its equality duty and that, as far as is practicable, this document is free from having a potential discriminatory or adverse/negative impact on people or groups of people who have relevant protected characteristics, as defined in the Equality Act of 2010.

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

DH	Department of Health
ISP or ISA	Information Sharing Protocol or Agreement. This is an agreement or a written process which defines the purposes and arrangements for sharing information with third parties.
Personal Identifiable Data/ Personal Identifiable Information (PID)	Personal Identifiable Data (PID) is information (an identifier) about a person from which the individual could be singled out (identified)
Information Asset	An information asset is a body of information which is defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. An Information Asset is organized Information that is valuable and easily accessible to those who need it.
Safe Haven	Safe Haven is a set of procedures which act as a safeguard for confidential information which enters or leaves the organisation, whether this is by facsimile (fax), e-mail, post or other means.

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
Caldicott Guardian	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 (see Appendix 1). The Caldicott Guardian is the Medical Director.
Information Governance Manager	The IG Manager has the day to day responsibility for implementing and monitoring safe haven guidance and thus ensuring the security of personal information in data transfers.
Senior Information Risk Officer (SIRO)	The SIRO has overall responsibility for information risk within the Trust. The role includes briefing the board and providing assurance through the 'Statement of Internal Control' that the information risk approach is effective in terms of resource, commitment and execution. The Trust SIRO is the Director of Corporate Development, Governance and Assurance
Managers and Supervisors	All managers, team leaders and supervisors (or deputy) are responsible for ensuring that all staff within their sphere of responsibility are familiar with this policy and other IG policies and procedures including the Data Protection and Confidentiality policy and the Information Incident Management procedure. They are to ensure that the appropriate modes transfer are implemented and embedded in their work processes or areas of authority.
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 • Ensure they comply with local safe haven policies and procedures. All staff should promote good practice and notify their line managers if the procedures are not being followed.

7. SUBSTANTIVE CONTENT

According to the DH, the key safe haven principles are:

- Each organisation should establish safe haven administrative arrangements to safeguard confidential person identifiable information. This includes having one designated contact point per physical site. All information exchanged between organisations should strive to pass between safe haven contact points
- All members of staff should be made aware, at least in general terms of the policies and procedures surrounding safe haven access
- Safe haven procedures should be fully documented and approved by the Caldicott guardian and agreed by senior management
- All staff have a professional responsibility for the information they send outside of the Trust and must think carefully about the method used to communicate such information.

It is vital that staff choose the most appropriate method of communication based on factors such as:

- The sensitivity of the information
- The urgency of the need to share information
- The operating procedures of the receiving organisation
- The reason for sending the information

Staff must not base their choice of communication on ease for them; whilst sending a fax may be convenient and quick, would that information be better safeguarded if it were communicated by telephone or secure email?

7.1. Safe Haven Locations in the Trust

There is an officially designated safe haven area within the Trust, located in the Information Department's Office on the first floor of the main block (Area T) at Billing Road.

Other areas in the Trust that are suitably secure and to which patients, members of the public and unauthorised staff do not have access could be made a safe haven provided that staff are trained and knowledgeable of their obligations. The following areas are accredited with safe haven status: Medical Records, Pathology Departments, Radiology Records, Pharmacy department and the Post Room.

7.2. Clear Desk

The Trust operates a "clear desk policy" whereby:

- All personal information must be stored securely and not left in view of others. Appropriate measures need to be implemented on a local basis to ensure that no records are left unattended or in a manner where they may be seen by unauthorised persons, including members of staff. All paperwork should be securely locked away outside of working hours.

- PC display screens and monitors must be facing away from walkways and public areas. PCs in reception areas must be sited at desks with the screen facing a wall whenever possible

7.3. Telephone Calls

- Try to avoid leaving a message
- You should always confirm the name, job title, department and organisation of the person requesting information
- Confirm the reason for information being requested if appropriate
- Where appropriate, take a contact number from the person making this request e.g. a main switchboard number; this is to guard against people seeking information by deception, so never take a mobile telephone number
- Telephone this number to test it is the correct number
- If you are unsure, check with your line manager whether information can be provided. If you remain in any doubt as to whether you can disclose the information, tell the enquirer you will call them back and seek assistance from the Information Governance Manager (ext. 3881)
- When you are satisfied with the enquirer's identity and right to access, only provide this to the person requesting
- Recorded telephone messages containing personal information must be received into a secured, password protected voicemail to mitigate the risk of unauthorised access to the message.

7.4. Sending and Receiving Emails

- Email should not be used to send confidential information where the recipients are external to the Trust email system, unless the contents of the email are password protected or encrypted. For these purposes the Trust email system means email addresses ending in @ngh.nhs.uk
- Emails containing PID which are to be sent externally and are not otherwise encrypted must use the nhs.net email system. Email addresses that end in @nhs.net are a secure method of transmission of patient information but only if both the sender and recipient has an nhs.net account or if sending to another government secure domain such as:
    - GSi (*.gsi.gov.uk);
    - CJX (*.pnn.police.uk);
    - GSE (*.gse.gov.uk);
    - GSX (*.gsx.gov.uk);
    - GCSX (*.gcsx.gov.uk);
    - SCN (*scn.gov.uk);
    - CJSM (*cjsm.net);
    - MoD (*.mod.uk).

- For employee confidential correspondence and other Human Resources functions, the individuals should be informed where encryption and NHS.net are not possible.
- No personal information should be contained in an email subject line. This includes name, date of birth and NHS or local hospital number.
- Emails containing PID should contain 'Confidential' in the subject line.
- Confidential information must not be sent by staff to personal email accounts. This includes hotmail, googlemail and doctors.net.

Emails containing confidential information should use the appropriate safeguards, namely:

- Clinical information must be clearly marked
- Emails addresses are checked so information is sent to the right people
- Delivery and read receipts options are checked to verify the message has been successfully sent and to confirm the recipient has read it
- Internet browsers are safely set up so that, for example, passwords are not saved and temporary internet files are deleted on exit
- Information sent by email must be safely stored and archived as well as being incorporated into patient records
- Patient or confidential Trust information is not saved or copied onto any personal PC or media that either does not belong to the Trust or is not approved by the Trust.

7.5. Sending and Receiving Post

The appropriateness of sending an item by special delivery needs to be balanced against the risk of any confidentiality breach and the practical and economic issues of recorded delivery.

- No unencrypted personal identifiable information should be transferred outside the Trust without prior board approval. This can be applied for through the Information Governance department.

The following safeguards should be followed for all types of post:

- Confirm the name, department and address of the recipient
- Ensure that the information is placed in a sealed robust envelope (for both internal and external post)
- Ensure that the name and address of the recipient is clearly marked
- Mark the envelope "Private and Confidential for Addressee only"
- No Trust logos or identifiers should be visible on envelopes
- If using a courier bag ensure that the courier bag is addressed to a named recipient; if the courier bag contains information for multiple addressees ensure that all information contained within the courier bag is in sealed addressed envelopes
- When necessary ask the recipient to confirm receipt of post
- Incoming mail must be opened away from public areas

7.6. Transfer of Medical Records within the Trust

Dedicated Medical Records Clerk/Porters deliver and collect case-note folders throughout the Trust. They receive training in the safe handling of medical records and follow specific procedures for the safety and confidentiality of records in transit.

In addition all staff should adhere to the following practices in order to assist in the safe and prompt transfer of records:

- Transportation vehicles holding patient records may be left for a short time in secure areas where only authorised staff can gain access whilst Medical Records staff deliver records to less accessible areas.
- Patient information must not be visible whilst transporting records.
- All staff should assist in the safe delivery of patient records by providing easy access for Medical Records staff to all areas of the hospital.
- It is the responsibility of Departmental and Ward Managers to ensure patient confidentiality by providing a secure area for the storage, collection and delivery of patient records in their areas.
- In the interests of patient care, it may be necessary for the patient to transport his/her notes around the Trust. The notes should always be in sealed envelopes, and the patient must sign a receipt. Patient's should not be allowed access to their record during transit

7.7. Using Couriers

- If material containing personal information or other confidential information is to be transported via courier, an E-procurement order form must be completed with an appropriate Trust authorisation.
- The materials to be couriered should then be passed to the Procurement department for action. The Procurement department will use an authorised courier.
- For regular courier transfers, arrangement should be made with the Procurement department so that the requesting department can deal directly with the couriers.
- For departments where the cost for transportation is covered by a third party or the courier service is prepaid; it is the department's responsibility to ensure that a reputable company is being used for the transfer.
- Personal information should not be sent via taxi unaccompanied by a member of staff without a prior exemption from the Caldicott Guardian on behalf of the Trust Board. This can be obtained by contacting the Information Governance Manager.

7.8. Fax Machines

- Confidential information held by the Trust should only be sent by fax where it is absolutely necessary
- Ensure that fax machines are located in safe havens locations at both ends of the transmission
- Anonymise the information wherever possible
- Always double check the fax number that you are sending information to-

- Use pre-programmed numbers where possible to avoid misdialling; however ensure that pre-programmed numbers are still checked regularly to ensure they are current
- Contact the recipient before sending to let them know you will be sending the fax
- Ask the recipient to acknowledge receiving the fax immediately
- Use the fax cover sheet - see Appendix 2
- Always request a report from the fax machine to confirm transmission was successful
- Personal details should be faxed separately from clinical details. Clinical details should be sent using the NHS number and no other patient identifiable information should be included

7.9. Holding information electronically

- Patient or Trust sensitive information must be held on the Trust's network servers (shared drives) and must not be stored on local hard drives or desktops
- Access to shared drives must be monitored by the drive administrator

7.10. Using USBs or other portable media

- No external device or equipment, including discs, USB drives and other data storage devices, should be run on or connected to NGH systems without the prior notification to and approval of the IT department
- When transferring information on portable media ensure the device is encrypted. Encrypted USB drives containing personal information must be used whilst on Trust premises and also for external use/ transfers (contact the IT Helpdesk for assistance).

7.11. Remote Working

Remote workers must:

- Password protect any work which relates to NGH business so that no other person can access the work
- Be so positioned to ensure that work cannot be seen by any other person whom it does not concern
- Take reasonable precautions to safeguard the security of Trust equipment, and keep passwords secret
- Inform the police and the Trust IT department (as appropriate) as soon as possible if either Trust equipment in your possession, or any computer equipment on which Trust work is undertaken, even if this is personal IT equipment, has been lost or stolen; and
- Ensure that any work undertaken remotely is saved on a NGH system or is transferred to NGH systems as soon as reasonably practicable.

7.12. Transporting bulk personal information

Bulk information is defined as 10 items of personal identifiable data or more but also includes fewer records where the information is particularly sensitive, i.e. sexual health, or the information being sent has the risk of identity fraud i.e. DBS forms.

- Bulk personal identifiable information should only be taken off site when absolutely necessary e.g. when clinics are being run off site.
- A register must be maintained detailing what information is off site, for what purpose and under who's responsibility
- Information must be transported in sealed containers and stored in a secure location.
- Never leave personal identifiable information unattended
- Ensure the information is returned back on site as soon as possible

7.13. Information Sharing Protocols/Agreement

When personal information is routinely shared with a third party, an Information Sharing Protocol should be established. These provide assurance in respect of the standards that each party to an agreement will adopt. New and revised sharing partnerships must be discussed with the Information Governance Manager to determine whether an ISP is required and as appropriate to establish the protocol.

7.14. Misconduct

The following matters will be treated as gross misconduct and the will be dealt with in accordance withthe Trust's Disciplinary Policy

- Repeated or negligent breaches of this policy
- Deliberate breach of this policy

8. IMPLEMENTATION & TRAINING

- Safe haven procedures are discussed at induction and published in Trust newsletters
- A supporting practice document will provide simple instructions on best practice for communications
- This policy is available on the Trust intranet, which can be accessed by all staff
- The policy will be distributed to all heads of departments who will disseminate to their team members

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
The safe haven practices as outlined in this policy.	Information Governance incidents, concerns, comments, complaints or disciplinary action that results as a breach of this policy	Information Governance Manager	There will be quarterly reviews of incidents or concerns	Information Governance Manager reporting to the Information Governance Group	Information Governance Manager	The Information Governance Group

10. REFERENCES & ASSOCIATED DOCUMENTATION

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/publications/the-nhs-constitution-for-england [Accessed 18 March 2016]

Department of Health (2010) Caldicott Guardian Manual 2010 [online] London. Department of Health. Available from: http://systems.hscic.gov.uk/infogov/links/2010cgmanual.pdf [Accessed 6 April 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://nww.igt.hscic.gov.uk/ [Accessed 24 February 2016]

Department of Health (2007) NHS information governance: guidance on legal and professional obligations. [online]. London: DH. Available from: https://www.gov.uk/government/publications/nhs-information-governance-legal-and-professional-obligations [Accessed 18 July 2016]

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

Human Rights Act 1989. (c.42). [online]. London: HMSO. Available from: http://www.legislation.gov.uk/ukpga/1998/42/contents [Accessed 7th April 2016]

Northampton General Hospital NHS Trust (2016) *Disciplinary*. 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) *Information Security Policy*. NGH-PO-011. 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) *Corporate documentation management policy: information lifecycle*. NGH-PO-123. Northampton: NGHT

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

Northampton General Hospital NHS Trust (2015) *Electronic mail and internet (including all social networking sites)*. NGH-PO-10-2. 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

Northampton General Hospital NHS Trust (2010) *Management of incidents (including serious incidents)*. NGH-PO-393. 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	**Caldicott principles**
Appendix 2	**Fax Cover Sheet**
Appendix 3	**Guidance for sharing personal information by Post Mail Flow Chart**
Appendix 4	**Guidance for sharing personal information by Telephone**
Appendix 5	**Guidance for sharing personal information by E-mail**
Appendix 6	**Guidance for sharing personal information by Courier**
Appendix 7	**Guidance for sharing personal information by Fax**

Appendix 1 Caldicott Principles

There are six Caldicott principles which govern how information should be share.

These are:
Principle 1 – Justify the purpose(s) for using confidential information

Principle 2 – Only use it when absolutely necessary

Principle 3 – Use the minimum that is required

Principle 4 – Access should be on a strict need-to-know basis

Principle 5 – Everyone must understand his or her responsibilities

Principle 6 – Understand and comply with the law

Appendix 2 **Fax Cover Sheet**

Urgent Fax

Date

Number of pages including cover sheet

TO:

Phone

Fax

CC:

REMARKS: *Urgent* ☐ *For your review* ☐ *Reply ASAP* ☐ *Please Comment* ☐

Dear

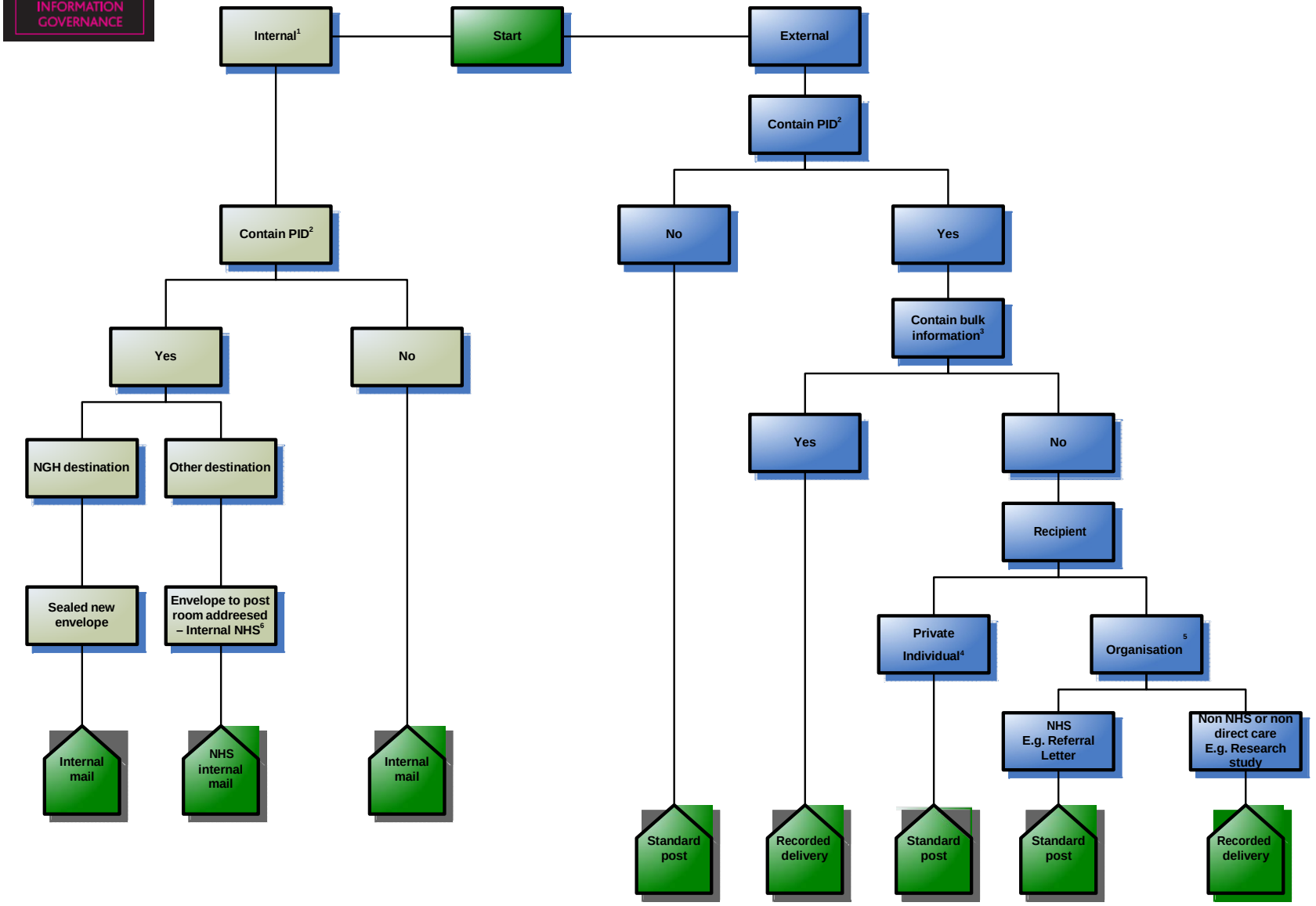
Please confirm receipt of this fax

Thank you.

Yours sincerely,

Appendix 3

Guidance for sharing personal information by Post Mail Flow Chart



Mail Flow Chart Explanatory notes:

The Mail flow is designed to assist in selecting the correct mail delivery system for the correspondences the Trust sends. The recommended outcomes are the *minimum* acceptable security.

Any variance from this process should be brought to the attention of Information Governance Department immediately

(1) The **Internal mail** system incorporates all NGH sites and local NHS sites including Doctor Surgeries. A full list of internal sites available is below

(2) **PID** is personal identifiable data, i.e. information that could be used to identify an individual.

(3) **Bulk information** is defined as *10 items* of personal identifiable data or more but also includes fewer records where the information is *particularly sensitive*, i.e. sexual health, or the information being sent has the risk of *identity fraud* i.e. CRB forms

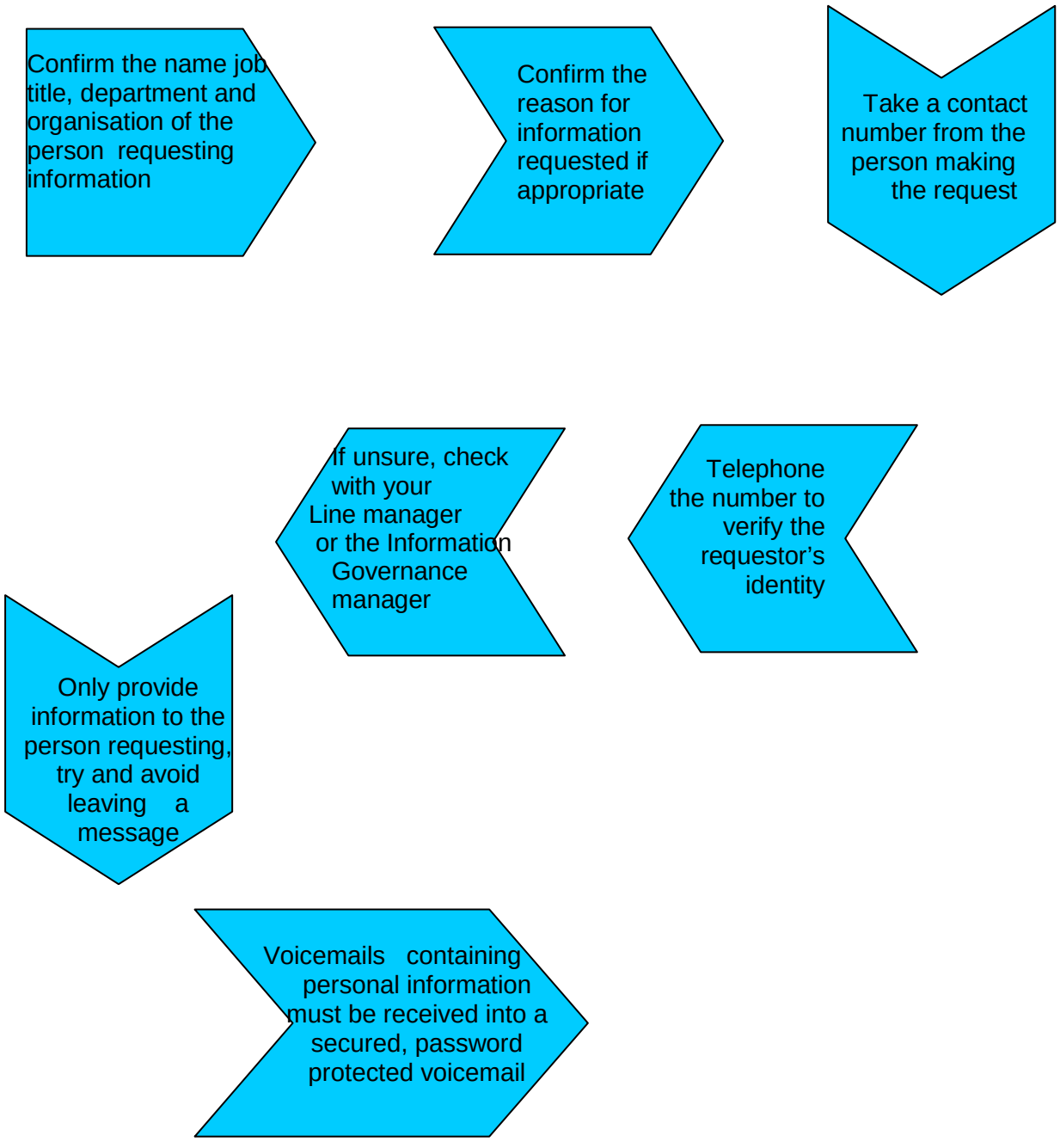
(4) **Private Individual** is defined as someone not associated with an organisation for the purpose of the communication. They are recipients for reason private to them and the Trust. This is to include patients and members of staff

(5) **Organisation** includes named individuals where the purpose of the correspondence is for professional reasons, i.e. referral letters, letter to GPs, letters to solicitors.

(6) **Envelope to post room addressed – Internal NHS** will ensure that the post room process the letter for delivery via the NHS mail delivery system.

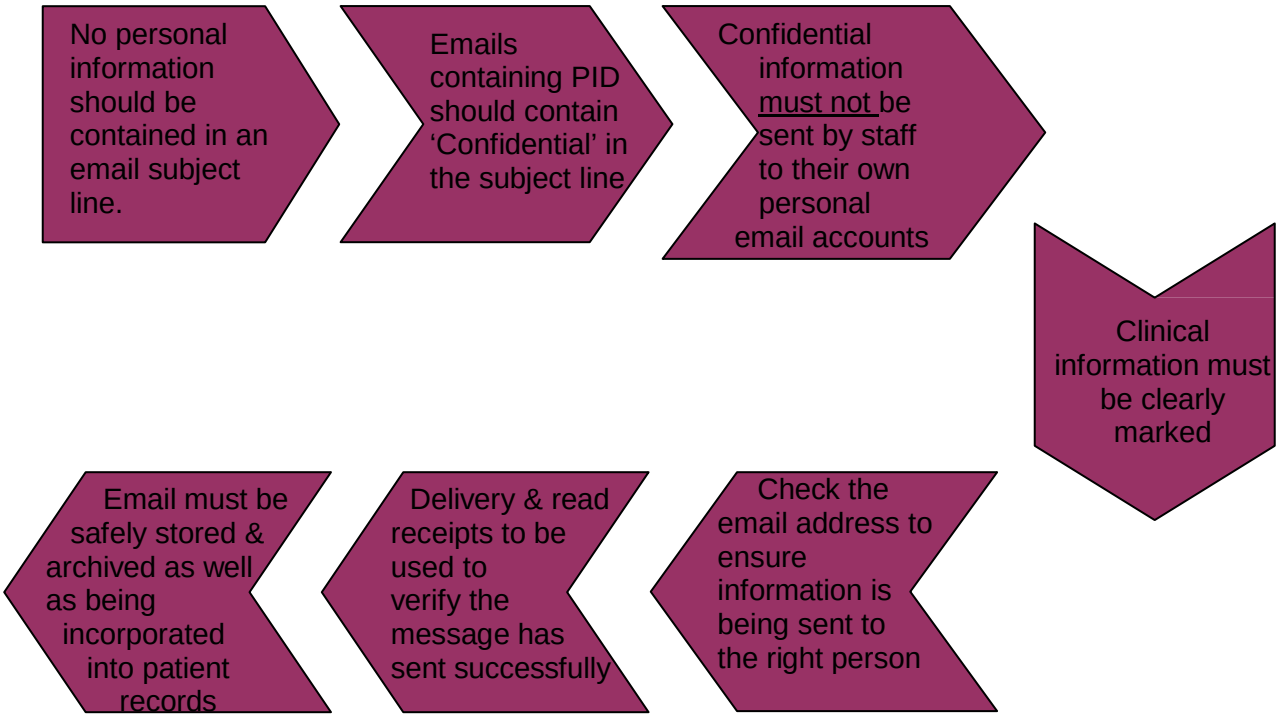
For further advice and guidance, please contact the Information Governance Department on ext. 3881 or dataprotectionact@ngh.nhs.uk

Guidance for sharing personal information by Telephone



Northampton General Hospital NHS
NHS Trust

Guidance for sharing personal information by E-MAIL



Emails containing confidential information which are to be sent externally and are not otherwise encrypted must use the @nhs.net email system.

Email addresses that end in @nhs.net are a secure method of transmission of patient information but only if both the sender and recipient has an nhs.net account or if sending to another government secure domain such as:

- GSi (*.gsi.gov.uk);
- CJX (*.pnn.police.uk);
- GSE (*.gse.gov.uk);
- GSX (*.gsx.gov.uk);
- GCSX (*.gcsx.gov.uk);
- SCN (*scn.gov.uk);
- CJSM (*cjsm.net);
- MoD (*.mod.uk)..

For other functions the individuals consent should be obtained where encryption and NHS.net are not possible i.e. Human Resources references.

Northampton General Hospital NHS
NHS Trust

Guidance for sharing personal information by COURIER

An E-procurement order form must be completed and authorised

Materials to be transported should be passed to Supplies (for one off transfers)

- For regular courier transfers, the requesting department can deal directly with the couriers.

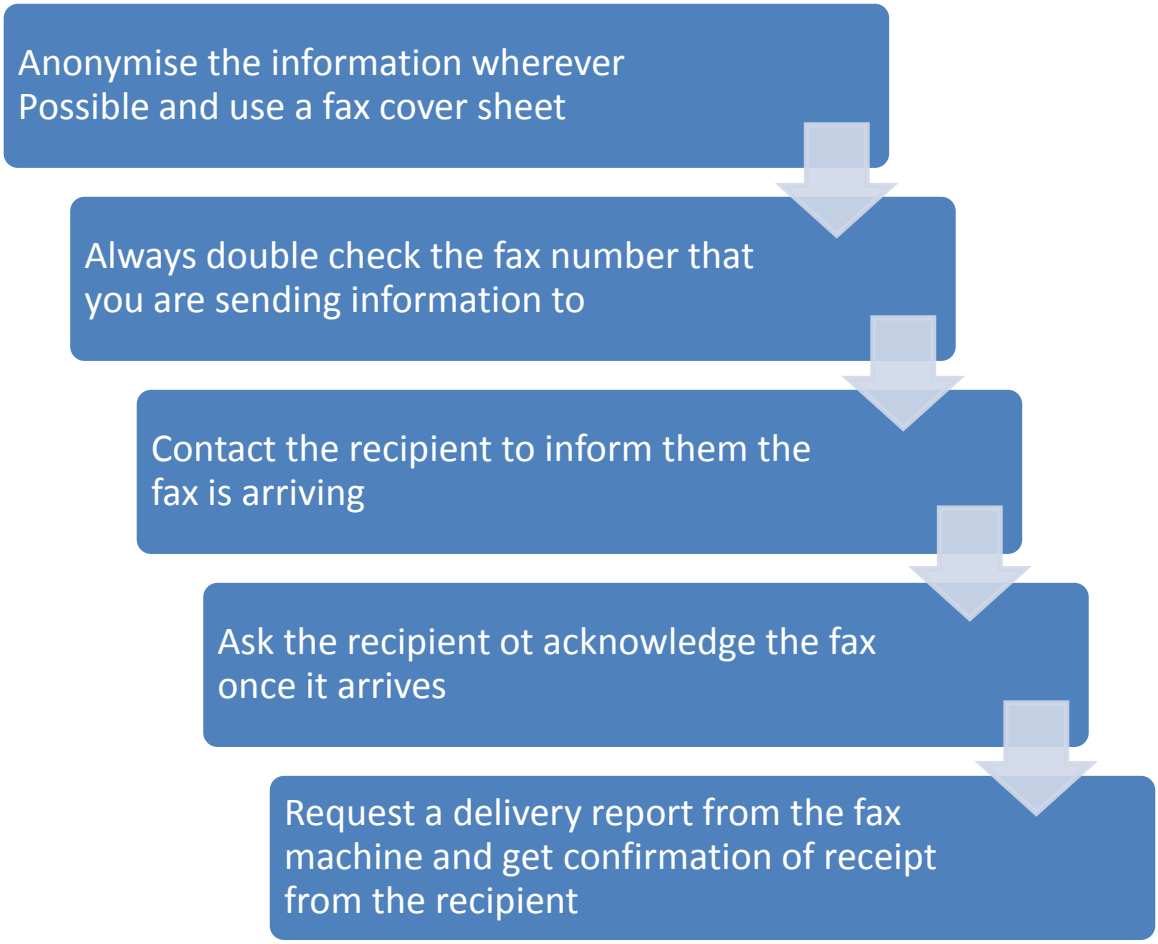
Supplies will use an authorised courier service

Personal Information must not be sent unaccompanied by staff via taxi

For departments where the cost for transportation is covered by a third party or the courier service is prepaid; it is the department's responsibility to ensure that a reputable company is being used for the transfer.

Northampton General Hospital NHS
NHS Trust

Guidance for sharing personal information by FAX



Confidential information held by the Trust should only be sent by fax where it is **absolutely necessary**.

Personal details should be faxed separately from clinical details. Clinical details should be sent using the NHS number and no other Patient identifiable Information should be included

FORM 1 & 2 - To be completed by document lead

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:	Transmission of Confidential Information (Safe Haven) policy
Is the document new?	No
If yes a new number will be allocated by Governance	New Number
If No - quote old Document Reference Number	NGH-PO-066
This Version Number:	**Version: 4**
Date originally ratified:	April 2014
Date reviewed:	June 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)	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, portable devices, encryption, safe haven, transmission

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

FORM 1 & 2 - To be completed by document lead

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	16 May 2016	Define some terms	Included
		7.12. Transporting bulk personal information. How could this be monitored? For example are doctors allowed to take patients notes in their own cars for meetings etc?	This is specifically for Bulk transfers. Clinics held off site have a different work process. Patients notes should always be tracked and this will serve as an information log as to where the records are going and who is responsible for them
Ben Leach	16 May 2016	None requested	N/A
Maxine Foster	16 May 2016	Inclusion of Pharmacy department as a safe haven	Included
Sue Campling	16 May 2016	Query on Sending and Receiving e-mails in respect of the Accessible Information Standard	Clarified
Fiona Barnes	16 May 2016	Query on Sending and Receiving e-mails in respect of the Accessible Information Standard	Clarified
Paul Gilliatt	16 May 2016	Rewording of section 2	Reworded

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	**7.7**
Monitoring	YES / NO	
Refs & Assoc Docs	YES / NO	
Appendices	YES / NO	

FORM 1 & 2 - To be completed by document lead

FORM 3- RATIFICATION FORM (FOR PROCEDURAL DOCUMENTS GROUP USE ONLY) **Read in conjunction with FORM 2**			
Document Name:		**Document No:**	**NGH-**
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**	Needs more information about the content of the Policy. 'Safe Haven' to be added.	Completed
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**	Old Equality and Diversity statement needs updating.	Completed
Definitions –is it clear what definitions have been used in the	**YES / NO / NA**	Need to remove 'Caldicott Guardian' as it is in roles and responsibilities Add PID to Personal Identifiable Data. Capitals. Remove Highlight off of Safe Haven	 Completed Completed
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**	7.3 To add as first bullet point 'Try to avoid leaving a message' 7.8 Appendix B changed to Appendix 2 7.14 'as outlined in' to be changed to 'in accordance with'	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 to be changed as recommended No Appendices 8 or 9 Not all Appendices are referenced throughout the document	Completed

Are the keywords relevant	**YES / NO / NA**		
Name of Ratification Group: Procedural Documents Group	**Ratified Yes/No: Subject to minor amendments**	**Date of Meeting: 21/07/2016**	