DATA PROTECTION & CONFIDENTIALITY POLICY

NGH-PO-334

Ratified By:	Procedural Document Group
Date Ratified:	January 2015
Version No:	4
Supercedes Document No:	3.2
Previous versions ratified by (group & date):	July 2013 PDG
Date(s) Reviewed:	January 2015
Next Review Date:	January 2018
Responsibility for Review:	Information Governance Manager
Contributors:	Information Governance Manager

POLICY

CONTENTS

POLICY

Version Control Summary

Version	Date	Author	Status	Comment
4.0	26 November 2014	Louise Chatwyn – Information Governance Manager	Draft	Review and update
4.1	10 February 2015	Louise Chatwyn – Information Governance Manager	Draft	Incorporation of PDG comments

SUMMARY

All employees working in the Trust have an obligation to protect the confidentiality of person identifiable information that they may come into contact with during their duties for the Trust. This is not just a requirement of their contractual responsibilities but also a legal obligation under the Data Protection Act 1998

This policy outlines the obligations and principles for handling confidential information and thus provides a consistent and integrated approach to data protection. This policy applies to all individuals employed by the Trust, and working within or on behalf of the Trust; including contractors, voluntary workers, students, locum and agency staff.

1. INTRODUCTION

This policy is written to set out Northampton General Hospital NHS Trust's commitments to and responsibilities for data protection and confidentiality.

Data protection law exists to promote the rights of individuals in respect of privacy and transparency whilst allowing organisations to use data for legitimate business purposes.

The Data Protection Act 1998 is concerned with personal data about living individuals where that data is processed in any of the following ways:

- Obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including
  - Organisation, adaptation or alteration of the information or data
  - Retrieval, consultation or use of the information or data
  - Disclosure of the information or data by transmission, dissemination or otherwise
  - Making available, or
  - Alignment, combination, blocking, erasure or destruction of the information or data

Whilst for the deceased there are no clear legal obligations of confidentiality it is recognised by the Department of Health and General Medical Council that there is an ethical basis for requiring that confidentiality obligations must continue to apply after death. Access to records of deceased individuals is governed by the Public Records Act 1958 and the Access to Health Records Act 1990. This policy shall refer to living and deceased individuals jointly unless where stated as the principles of protecting the information shall be the same for both.

Further guidance on the protection and access requirements to health information of individuals is provided by the Confidentiality: NHS Code of Conduct and the Caldicott principles which are formed from the Caldicott Report.

This policy has been produced to notify staff of their responsibilities for protecting information with respect to the data protection and confidentiality, so that they do not inadvertently breach any of the requirements.

This policy should be read in conjunction with the Trust's Transmission of Information (Safe Haven) policy, Information Security policy and Information Incident Investigation Protocol

2. PURPOSE

The Purpose of this document is to:
Outline the legislation and guidance that governs the processing of person identifiable information.

- Promote good practice to all staff and advise them of their responsibilities in the use and disclosure of information. This will minimise the risk faced by staff in processing information in accordance with their duties for the Trust.

- Apply the principles of safeguarding personal information to the safeguarding of confidential business and non-personal information
- Assist the Trust in meeting its statutory obligations and standards of good practice, including the Information Governance Toolkit

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 process information including, but not limited to, health records, personnel files, email accounts and portable storage devices.
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. This to include where staff are employed by the Trust but may primarily work in the Community
e) All persons who use or have access to any of the above mentioned in 3 a), 3b), 3 c) or 3 d) including substantive, locum, agency, bank staff. Volunteers and students may also come into contact with data falling within the remit of this policy and are therefore also covered.

4. COMPLIANCE STATEMENTS

Equality & Diversity

This policy has been designed to support the Trust's effort to promote Equality and Human Rights in the work place and has been assessed for any adverse impact using the Trust's Equality Impact assessment tool 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 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 Principles and Values of the NHS along with the Vision and Values of Northampton General Hospital NHS Trust.

5. DEFINITIONS

CCTV	Closed Circuit Television
DPA	Data Protection Act 1998

Data Controller	The Trust is the Data Controller for the purpose of the Data Protection Act 1998. As Data Controller the Trust must: • Maintain an up-to-date notification (registration) with the Information Commissioner's Office which details how the Trust will process varying categories of personal data • Ensure compliance with principles of the Data Protection Act 1998 • Ensure the development of relevant data protection practices are instigated within the Trust • Ensure that advice is readily available to staff on data protection issues • Ensure that breaches of the Act are investigated, reported as necessary and that learning outcomes are initiated across the Trust. The Information Governance Manager is the Trust's data controller representative
Data Subject	The person to whom identifiable information relates
FOIA	Freedom of Information Act 2000
ICO	Information Commissioners'' Office. The ICO regulate Data Protection laws in England
NGH	Northampton General Hospital NHS Trust
Third Party	Any person other than the individuals authorised to process data for a specified purpose by the data controller
SIRO	Senior Information Risk Owner. The Trust accountable officer

6. ROLES & RESPONSIBILITIES

ROLE	RESPONSIBILITY
Chief Executive and the Trust Board	Chief Executive and the Trust Board have ultimate accountability for actions and inactions in relation to this policy
Senior Information Risk Officer	The Trust's SIRO is responsible for having overall accountability for Information Governance in the Trust; this includes the Data Protection and Confidentiality function. The role includes briefing the board and providing assurance through the 'Statement of Internal Control' that the Data Protection and Confidentiality approach is effective in terms of resource, commitment and execution. The Trust's SIRO is the **Director of Strategy and Partnerships**

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. The Trust's Caldicott Guardian is the **Medical Director**
Head of Information and Data Quality	The Head of Information and Data Quality has overall day to day responsibility for the Information Governance in the Trust; this includes the Data Protection and Confidentiality function. The role includes briefing the executive team, including the SIRO and Caldicott Guardian of information risks and investigating information serious incidents
Information Governance Manager	The Information Governance Manager has day to day responsibility for implementing and monitoring procedures to ensure compliance with the Data Protection Act 1998, Confidentiality: NHS Code of Conduct and other relevant guidance thus ensuring the security of personal identifiable information The Information Governance Manager and their team are responsible for making available methods of accessing suitable training and carrying out training presentations
Managers	Managers and supervisors are responsible for ensuring that staff who report to them have suitable access to this policy and it's supporting documents and that the procedures in this policy and supporting documents are implemented in their area of authority. Managers are also responsible for ensuring the training compliance of all staff reporting to them
All Trust Employees	Have a responsibility to: • Support the Trust to achieve its Vision • Act at all times in accordance with the Trust values • Follow duties and expectations of staff as detailed in the NHS Constitution – Staff Responsibilities All staff have a responsibility to ensure they comply with local data protection and confidentiality policy. All staff should promote good practice and notify their line managers if the procedures are not being followed.

7. SUBSTANTIVE CONTENT

All employees working in the Trust have an obligation to protect the confidentiality of person identifiable information that they may come into contact with during their duties for the Trust. This is not just a requirement of their contractual responsibilities but also a legal obligation under the Data Protection Act 1998 and included in professional codes of conduct, including the NHS Standards of Business Conduct.

Employees are obliged to keep all person identifiable information strictly confidential. This includes patient and staff records. Furthermore, during their duties for the Trust, staff may also come into contact with business confidential information which should be treated with the same degree of protection as person identifiable information.

By adhering to good practice on data protection and confidentiality, staff will help to promote a secure environment where both patients and staff can feel confident that person identifiable information is being handled professionally, appropriately and in accordance with the law. By applying the same principles to non-personal confidential information, this will protect NGH as a business and ensure it is able to conduct its legitimate activities without prejudice or interference.

Further detail surrounding the Data Protection Act is available from the Information Commissioners Office which is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

7.1. Data Protection Act Principles

In accordance with the Data Protection Act 1998 it is the duty of the Trust to comply with the data protection principles in relation to all personal data to which it is the data controller. There are 8 principles in the Data Protection Act 1998. The Trust shall ensure compliance with the principles as follows:

7.1.1. First Principle

Personal data shall be processed fairly and lawfully

The Act requires that certain conditions must be met for the legal processing of data to take place. These conditions are listed in Schedule 2 (personal data) and Schedule 3 (sensitive data) of the Act and in Appendix 1 of this policy.

When collecting person identifiable data, the Trust must make readily available the following:

- The identity of the Trust as the collector of the Information.
- The identity of the Information Governance Manager as the nominated individual acting on behalf of the Trust as data controller.
- The purpose for which the data will be processed.
- Any other information to ensure that individuals are fully aware of how their information will be used.

Patient and staff information leaflets and fair processing statements are available which detail how information is obtained, processed and protected.

7.1.2. Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

The Trust must register its uses of personal information with the ICO in the form of a data protection notification. The Trust's notification includes purpose description, data subjects, data classes, sources and disclosures (recipients) and where the information is sent to.

Compliance with this principle will be achieved by:

- The Information Governance Manager ensuring that the Trust's notification is up-to-date and accurate of the practices undertaken by the Trust. Notification must be updated on an annual basis. The register is publicly available and can be searched at the following website address http://ico.org.uk/what_we_cover/register_of_data_controllers
- Departmental audits, undertaken by the Information Governance Manager, will ensure that information is only used for the purpose it was obtained for

7.1.3. Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

Compliance with this principle will be achieved by:

- Only information that is required for the specific purpose of processing is collected
- New projects which collect data are reviewed by the IM&T Subcommittee to ensure that the data is not unnecessarily collected. A Privacy Impact Assessment will be undertaken as instructed by the IM&T Subcommittee for projects where personal information is used in new or alternative ways to current practice.

7.1.4. Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

Compliance with this principle will be achieved by:

- Patient details are checked at the start of every hospital episode to ensure the records held are accurate
- Validation procedures are implemented to check and maintain staff and patient person identifiable information.
- Data quality is subjected to appropriate levels of audit.

7.1.5. Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Compliance with this principle will be achieved by:

- The Trust will ensure that the guidelines set out in the Department of Health Records Management: NHS Code of Practice, in the Trust's Non Health Records Management policy and the Management of Health Records policy for the retention and destruction of documents are followed

- Regular reviews of information are undertaken to identify when the information is beyond its minimum retention term and is no longer required.

7.1.6. Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The Act gives 7 key rights to the data subject:

- The right to access information held about them (subject access)
- The right to prevent processing that is likely to cause harm or distress
- The right to prevent processing for the purpose of marketing
- The right to request manual intervention on decision making
- The right to take action for compensation if the individual suffers actual damage
- The right to take action to rectify, block, erase or destroy inaccurate information
- The right to make a request to the Information Commissioner's Office for an assessment to be made as to whether any provision of the Act has been contravened

Compliance with this principle will be achieved by:

- Ensuring that appropriate procedures and policies are in place to respect the rights of individuals
- Ensuring that staff are adequately informed of individuals' rights
- Ensuring that procedures are in place to meet statutory deadlines in regards to responding to subject access requests
- Ensuring that data subjects are aware of their rights by promoting these to individuals through various mediums

7.1.7. Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Compliance with this principle will be achieved by:

- Maintaining procedures and operations to protect personal data from corruption, accidental loss or damage.
- Maintaining data transmission procedures to secure information in transit. The Transmission of Information (safe haven) policy details how information must be secured.
- Where breaches of this principle do occur, learning outcomes must be shared and initiated throughout the Trust to prevent future occurrences.

7.1.8. Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Compliance with this principle will be achieved by:

- Routine reviews of the Trust data mapping to identify transfers to the EEA and outside this zone

- Reviews of data transfers to identify where risks persist and how these can be reduced

7.2. Caldicott Function

In the early 90s, there was a big increase in patient records being held on computer systems. Clinicians wanted to keep control of records that were traditionally kept private between them and the patient. Clinicians were generally nervous about computer staff being able to see sensitive data. At the same time, computerised records encouraged researchers and academics to ask for more information about the clinical effectiveness of the health sector.

The Caldicott Committee was set up to maintain clinical control over patient records. They recommended that each health or social care organisation should appoint a Guardian of patient data, a Caldicott Guardian.

At NGH the Caldicott Guardian is the Trust's Medical Director.

There are 7 Caldicott Principles to govern how personal confidential information should be used and accessed. 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
Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality

The Trust Caldicott Guardian will ensure compliance with these principles by:

- Overseeing and approving protocols and procedures where confidential patient information may be shared with external bodies both within and outside the NHS, acting as the conscience of the organisation and enabler of appropriate and secure information sharing. This includes flows of information to and from partner agencies, sharing through NHS IT systems, disclosure to research interests and disclosure to other agencies e.g. the police.
- Championing confidentiality issues at board level.
- Assessing the risk of information breaches through the Serious Incident Group and ensuring that appropriate action is taken which may include notifying data subjects or the Information Commissioner.
- Ensuring that staff which routinely disclose information to third parties are suitably trained to identify genuine requests and to release the minimum required for the purpose.
- Overseeing confidentiality strategy initiatives.

Day to day responsibility for meeting these objectives lies with the Information Governance Manager who will provide assurance by:

- Reporting incident to the Serious Incident Group for review and maintaining effective information breach management procedures.

- Providing monthly reports to the Head of Information and Data Quality and the Caldicott Guardian outlining confidentiality risks and issues.
- Undertaking mandatory information governance training for staff across the Trust.
- Ensuring that data protection and confidentiality policies and procedures are up to date and fit for purpose.
- Conducting departmental audits to ensure that procedures are suitable and are being followed.

The Trust uses the Caldicott principles as a basis for appropriate access and disclosure of business confidential information. A breach of these principles for non-personal information will be classified as unauthorised access or disclosure.

7.3. Confidentiality

Individuals have a right to confidentiality under common law in that information provided in confidence must generally be handled in confidence and information obtained for one purpose should not be used for another without the consent of the subject.

Additionally, the Confidentiality: NHS Code of Conduct provides guidance for those who work within or under contract to the NHS.

Confidential information may be known or stored on any medium. Photographs and videos for example are subject to the same requirements as data stored in paper (hard copy) records or electronically.

Compliance with confidentiality obligations including the Confidentiality: NHS Code of Conduct will be achieved by ensuring that:

- Person-identifiable information is recorded accurately and consistently
- Person-identifiable information is not inappropriately disclosed
- Person-identifiable information is kept physically secure
- Person-identifiable information is used and disposed of with appropriate care. All confidential waste must be disposed of in confidential waste. The confidential waste sacks must be kept in secure areas, including when awaiting collection.
- Patients are made aware that the information they provide may be recorded
- Patients are aware that information may be shared in order to provide them with the best possible care
- Staff respect the rights of individuals and can assist them in exercising their rights to access

7.4. Fair Processing

Fair processing is the term applied to informing service users how their information is processed and for what specific purpose, including when their information may be shared with a third party.

The Trust has two fair processing notices; one for staff information and one for patient information. (appendix 1 and 2)

The staff fair processing statement is made available on application to the Trust along with the job description and personal specification. A copy is also held on the Trust Intranet.

The fair processing statement for patients is prominently displayed across the Trust and a copy is available on the Trust's public facing website.

7.5. Information Sharing

In order to share information certain conditions must be met. The sharing must be in accordance with the Caldicott principles, specifically, only when it is necessary, the recipient has a need to know and only the minimum information to satisfy the purpose is shared. Information that can identify the individual must only be shared if anonymisation is not suitable to the purpose of the information sharing.

The data subject should be informed of the intention to share unless this could unacceptably increase the risk posed to them. This would most likely only apply in cases of safeguarding or vulnerable patients.

Once informed, the data subject should consent and this consent documented in the Health Record. If a data subject with the capacity to consent refuses consent, it is likely that continuing to share their information would breach the Data Protection Act. The wishes of the data subject must be followed at all possible times.

Individuals can share confidential information without consent if it is required by law, or directed by a court, or if there is public benefit which outweighs both the public and the individual's interest in keeping the information confidential. Individuals must weigh the harm that is likely to arise from not sharing the information against the possible harm, both to the person and to the overall trust between doctors and patients of all ages, arising from releasing that information. This applies to safeguarding children and vulnerable adults. Each case should be assessed on its own merits and recorded in the notes. Information Governance or the Caldicott Guardian must be consulted if there is any uncertainty. Data Protection is not a barrier to sharing information but provides a framework to ensure that personal information is shared appropriately

7.6. Disclosure

A patient's health records are made by the health service to support that patient's healthcare.

Patients must be made aware of information disclosures that are necessary to provide them with high quality care. These disclosures may be where information is shared between members of care teams and between different healthcare providers including non-NHS organisations.

Patients generally have the right to object to the use or disclosure of confidential information that identifies them, and should be made aware of this right. However if a patient objects it might, in exceptional cases, limit the care or treatment options available. Patients must be informed if their decision about disclosure has implications for their care or treatment.

Provided patients have been informed of:

- how information relating to their healthcare will be used and disclosed
- the choices they have in relation to that use and disclosure
- the implications of opting to limit how that information may be used or shared

- Their explicit consent is not usually required for the information disclosures needed to provide their healthcare, as consent is taken to be implied in their agreement to examination and treatment.

Opportunities should nevertheless be taken to check that patients understand what may happen.

Consent cannot be assumed in cases where the purpose of the disclosure is not directly concerned with individual patient healthcare.

Information provided in confidence should not be used or disclosed for purposes other than healthcare without the individual's explicit consent or where there is a clear public interest or legal justification for doing so.

The exceptions to this rule are where there are statutory grounds for disclosing it; some of these grounds are listed in *Confidentiality: NHS Code of Practice* Annex C.

7.7. Unauthorised Disclosure

Employees of NGH and its partners will come into contact with confidential information of both a personal and business confidential nature.

The disclosure of information to any third party, including another member of staff, a private individual, another organisation or the data subject, without the authorisation from suitable line management may be classified as unauthorised and in breach of this policy

7.8. Unauthorised Access

Employees of NGH and its partners may have access to confidential information of both a personal and business confidential nature.

The access, or attempted access, to any information without a genuine business need may be classified as unauthorised and in breach of this policy. This includes access to the records of patients when not involved in the care of the patient.

Access to the Summary Care Record will be monitored by the designated Privacy Officer. Any self-claim legitimate relationships or access without patient consent will be investigated to ensure the access was appropriate. Unauthorised access to the Summary Care Record may be classed as a breach of this policy.

If members of staff wish to access their own medical records, this must be through the formal request process – in writing to the medical records department. Access to your own information not through the formal process is unauthorised and may be classified as a breach of this policy

7.9. Misconduct

Breaches of confidentiality are a serious matter and non-compliance with the Trust's policies and guidance may be considered as gross misconduct therefore rendering the individual liable to disciplinary action which could result in summary dismissal in accordance with the Trust's Disciplinary Policy.

In cases of reckless, deliberate, repeated or negligent misconduct the Trust holds the right to consider and take additional appropriate legal action which could lead to prosecution under the relevant legislation. This legal action includes sharing information with the Police.

7.10. Whistleblowing

Whistleblowing is when a person raises a concern, in the public interest, about wrongdoing occurring in an organisation or body of people. Usually this person would be from that same organisation. This Data Protection and Confidentiality policy is not an obstacle to whistleblowing and confidential information can be disclosed to the named parties in the Trust Whistleblowing Policy in relation to a whistleblowing concern.

It should however be considered whether personal information of a third party, in particular a patient, is required to be disclosed. It may be possible to raise the concern and explain circumstances without identifying third parties. Unless the identification of third parties is essential to the raising of the whistleblowing concern, identification should be avoided.

The Trust policy in this respect is detailed in Section 10 – Associated Documentation

7.11. Anonymised and Pseudonymised Information

Anonymised information does not identify an individual directly and cannot reasonably be used to determine identity. Anonymisation requires the removal of identifiers that in isolation or in combination with other identifiers might allow an individual to be recognised. This can include name, address, full post code, date of birth and NHS Number. Removal of patient name and address only does not automatically mean that the data is anonymised.

Pseudonymised information has individual identifiers removed and replaced with a code. The code allows for data recorded on an individual to be linked without the identity of the individual being disclosed.

Anonymised information is suitable for one-off requests or for identifying isolated incidents. Anonymised data should be requested and issued as standard unless the requestor can justify a need for pseudonymised or identifiable data.

7.12. CCTV

Closed Circuit Television cameras capture information and must therefore comply with relevant legislation including the DPA.

The use of CCTV at NGH is advertised by clear posters across the Trust and at the locations of the CCTV cameras. All cameras are in prominent positions and do not infringe on treatment areas.

CCTV images are automatically recorded and maintained for a maximum of 30 days, unless a request is received to hold a particular recording for longer.

CCTV is used for the purpose of crime prevention, prosecution of offenders and for the safety of staff and the general public. Images may be disclosed to third parties, including the Police, if it is compatible with this purpose. CCTV is subject to the FOIA. Requests for images will be processed in accordance with the Data Protection Act 1998 and Freedom of Information Act 2000.

8. IMPLEMENTATION & TRAINING

- Data protection and confidentiality procedures are discussed at induction and published in Trust newsletters.
- Information governance is included in the Trust's mandatory training policy.
- All employees have a confidentiality clause in their signed contracts obliging them to comply with confidentiality practices.
- 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
Staff will comply with guidance on safeguarding information as outlined in this policy	An annual data protection and confidentiality audit programme will review compliance with the principles. Learning outcomes and actions will be enforced as appropriate.	IG Manager	Ongoing Annual Program	IG Leads Board	IG Manager	IG Leads Board
Staff will be trained on data protection and confidentiality procedures at corporate induction sessions	Review of training attendance lists and departmental training compliance rates	IG Manager	Monthly	IG Leads Board / Mandatory Training Leads group	IG Manager	IG Leads Board / Mandatory Training Leads group
Staff will undertake annual information governance training which incorporates data protection and confidentiality in accordance with their job role training needs assessment	Review of training attendance lists and departmental training compliance rates	IG Manager	Monthly	IG Leads Board / Mandatory Training Leads group	IG Manager	IG Leads Board / Mandatory Training Leads group
Staff access to records will be authorised and only when necessary	Review of alerts generated	IG Team	Monthly	IG Manager	IG Manager	IG Leads Board

10. REFERENCES & ASSOCIATED DOCUMENTATION

Access to Health Records 1990 (C.23) [Online] London, HMSO. Available from: http://www.legislation.gov.uk/ukpga/1990/23/contents [accessed 17th December 2014]

Data Protection Act 1998 (c.29) [online] London, HMSO. Available from: http://www.legislation.gov.uk/ukpga/1998/29/contents[accessed 17th December, 2014]

Department of Health (2010) *Caldicott Guardian Manual 2010* [online] London. Department of Health. Available from: http://webarchive.nationalarchives.gov.uk/20121113092627/http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/2010cgmanual.pdf/view [accessed 17th December, 2014]

Department of Health (2003) *Confidentiality: NHS Code of Practice* [online] London. Department of Health. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf [accessed 17th December, 2014]

Department of Health (2006) Records Management: *NHS Code of Practice part 1* [online] London. Department of Health. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200138/Records_Management_-_NHS_Code_of_Practice_Part_1.pdf [accessed 17th December, 2014]

Department of Health (2009) Records Management: *NHS Code of Practice part 2* [online] London. Department of Health. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf [accessed 17th December, 2014]

National Information Governance Board (2011) *Care Records Guarantee.* Version 5. [Online] Available from http://webarchive.nationalarchives.gov.uk/20130513181011/http://www.nigb.nhs.uk/guarantee/pubs/nhscrg.pdf [accessed 17th December, 2014]

Northampton General Hospital NHS Trust (2014) *Disciplinary Policy.* Northampton, NGHT http://srv-wap-001/IG_DocControl/HG_ViewDoc.aspx?HG_DocID=d8427401-44a9-4f2b-8d6d-e6f010f2eaf4 [accessed 17th December, 2014]

Northampton General Hospital NHS Trust (2014) *Information Incident Investigation Protocol.* Northampton, NGHT http://srv-wap-001/IG_DocControl/HG_ViewDoc.aspx?HG_DocID=e49fbbec-8009-494f-964e-e74a49496511 [accessed 17th December, 2014]

Northampton General Hospital NHS Trust (2014) *Information Security Policy.* Northampton, NGHT http://srv-wap-001/IG_DocControl/HG_ViewDoc.aspx?HG_DocID=11f2a5d8-0685-4a23-95c3-d2bb0a38b26d [accessed 17th December, 2014]

Northampton General Hospital NHS Trust (2014) *Health Records Management policy.* Northampton, NGHT http://srv-wap-001/IG_DocControl/HG_ViewDoc.aspx?HG_DocID=98795b4f-08b3-4127-bede-52de8346b767 [accessed 17th December, 2014]

Northampton General Hospital NHS Trust (2014) *Corporate Documentation Management (Information Lifecycle) Policy.* Northampton, NGHT http://srv-wap-001/IG_DocControl/HG_ViewDoc.aspx?HG_DocID=39552bf7-d46e-4dc8-91c3-7149c8988558 [accessed 17th December, 2014]

Northampton General Hospital NHS Trust (2012) *Safeguarding Children Policy.* Northampton, NGHT available from http://srv-wap-001/IG_DocControl/HG_ViewDoc.aspx?HG_DocID=d5a4aa41-c0e0-44fd-8922-fd5e1501b56d [accessed 17th December, 2014]

Northampton General Hospital NHS Trust (2014) *Transmission of Information (Safe Haven) Policy.* Northampton, NGHT http://srv-wap-001/IG_DocControl/HG_ViewDoc.aspx?HG_DocID=85d5c919-bb28-4a40-9197-330f29607104 [accessed 17th December, 2014]

Northampton General Hospital NHS Trust (2013) *Raising Concerns at Work (Whistleblowing) Policy*, Northampton,NGHT http://srv-wap-001/IG_DocControl/HG_ViewDoc.aspx?HG_DocID=83d01881-3634-474e-8e17-e66204cae7fb [accessed 17th December, 2014]

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/170656/NHS_Constitution.pdf [Accessed 1 June 2013]

APPENDICES

Appendix 1 Fair Processing Statement – Staff

Northampton General Hospital NHS Trust (NGH) is registered to process personal and sensitive information under the Data Protection Act 1998 – registration number Z4694847.

Information collected during the recruitment process will be used to support your application to the Trust. The Trust may need to share your information with third parties such as previous employers, referees and government agencies to verify the information and confirm your suitability to work. Unsuccessful candidates will have any paper records disposed after an appointing decision has been made. Electronic information may be available through *NHS jobs* for up to 13 months after closing date.

Successful candidates will have their application details transferred to a personnel record and entered onto the Trust's electronic staff record, including Payroll. Personnel records will be maintained in accordance with the Department of Health Record Management Code of Practice.

Employee information is not shared with a third party without your consent unless there is a legal basis for disclosure; for example for the detection and prevention of crime or under the Social Security Administration Act 1992, or, if it is in the legitimate interest of the Trust, for example for contingency planning and disaster recovery. Employee information is processed for the purpose of maintaining a personnel record including attendance and performance.

All individuals have a legal right to access information held about them and can amend factually incorrect information. Anyone wishing to obtain a copy of their employee record or for further details on their information rights please contact the Information Governance team.

Information Governance
Northampton General Hospital
Cliftonville
NN1 5BD
01604 52 3881
dataprotectionact@ngh.nhs.uk

Appendix 2 Fair Processing Statement - Patients

Northampton General Hospital NHS Trust (NGH) is registered to process personal and sensitive information under the Data Protection Act 1998 – registration number Z4694847.

Northampton General Hospital collects key information on you, your medical conditions and clinical care. This information is maintained on your health record and may also be held electronically on computer systems. All information is held in accordance with the Principles of the Data Protection Act 1998 and all NHS staff has a legal duty to maintain your confidentiality.

The information about you is processed for the purpose of providing health care; this may include audit, training and protecting the health of the general public.

Northampton General Hospital may share information with other NHS providers or social care organisations for the purpose of ongoing care or treatment. We will also share information as required by law; for example, to comply with a court order.

We will anonymise your information wherever possible to protect confidentiality and we will obtain your consent prior to sharing, giving you the opportunity to object, wherever this is appropriate.

For further details contact the Information Governance team –

Information Governance
Northampton General Hospital
Cliftonville
NN1 5BD
01604 52 3881
dataprotectionact@ngh.nhs.uk

Providing the Best Possible Care

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:	Data Protection and Confidentiality
Is the document new?	**No**
If yes a new number will be allocated by Governance	N/A
If No - quote old Document Reference Number	NGH-PO-334
This Version Number:	**Version: 4**
Date originally ratified:	February 2009
Date reviewed:	January 2015
Date of next review: a 3 year date will be given unless you specify different	**January 2018 (3 Years)**
If a Policy has the document been Equality & Diversity Impact Assessed? (please attach the electronic copy)	**No**
DETAILS OF NOMINATED LEAD	
Full Name:	Louise Chatwyn
Job Title:	Information Governance Manager
Directorate:	Strategy & Partnerships
Email Address:	Louise.chatwyn@ngh.nhs.uk
Ext No:	3881
DOCUMENT IDENTIFICATION	
Keywords: **please give up to 10** – to assist a search on intranet	Data, Protection, Confidential, Breach, Caldicott

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
Induction and refresher training sessions	As per training sessions program detailed on intranet	IG Manager

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
PDG	23.12.2014		

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**
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	**Inclusion of Disclosure section**
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:	**Data Protection**	**Document No:**	**NGH-PO-334**
Overall Comments from PDG	**The document is written in 3rd and 1st person please check this throughout document.**		

	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	Please see comments in document – needs rewritten Delete flow chart as not relevant	Complete
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		
Definitions –is it clear what definitions have been used in the	YES / NO / NA	Include SIRO	Complete
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	Add whistleblowing policy reference	Completed – amended
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		
Are the keywords relevant	**YES** / NO / NA		

Name of Ratification Group:	**Ratified Yes/No:**	**Date of Meeting:**
Procedural Document Group	**Ratified subject to minor amendments and chair approval**	**15/1/2015** **Chair approved on 10/2/2015**