



Data Protection Policy

Document Profile Box	
Document Category / Ref	QSSD 1316
Version:	0002.1
Ratified by:	Policy Review Group Joint Consultative Committee
Date ratified:	15 th September 2009
Name of originator / author:	Rahima Hoque – Information Governance Manager
Name of responsible committee / individual:	Information Governance Working Group
Date issued:	31 st October 2009
Review date:	1 year from issue date
Target audience:	All staff
Document owner:	Colin Cessford – Director of Strategy & Business Development
Approved by:	

Version Control

Version	Release Date	Author	Status	Comments
0001	Feb 2008	Mark Glencorse	Final	First Issue.
0002	Apr 2009	Rahima Hoque	Draft	Revised in line with toolkit requirements. Renamed Data Protection Policy from Data Protection and Subject Access Policy. Subject Access Procedure and Form removed from appendix and contained in a separate document.
0002	Sept 2009	Rahima Hoque	Final	Following ratification.
0002.1	Nov 2009	Rahima Hoque	Final	Policy title in Docuviewer changed to match document title and document owner added to profile box.

Did you print this document yourself?

Please be advised that the Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version.

Document Location

The source of the document will be found in the Trust Quality System.

Freedom of Information Act 2000 Access

This document will be available via the NEAS Publication Scheme.

TABLE OF CONTENTS

	PAGE
1. INTRODUCTION	1
2. PURPOSE	1
3. SCOPE	2
4. DEFINITIONS	2
5. RESPONSIBILITY AND ACCOUNTABILITY	3
6. EQUALITY AND DIVERSITY STATEMENT	3
7. LEGAL AND PROFESSIONAL OBLIGATIONS	4
8. DATA PROTECTION ACT 1998	4
9. DATA PROTECTION PRINCIPLES	5
10. INFORMATION PROVIDED TO DATA SUBJECTS	7
11. INDIVIDUAL RIGHTS	7
12. SUBJECT RIGHTS	8
13. CONSENT	11
14. SECURITY OF DATA	11
15. RETENTION AND STORAGE OF CONFIDENTIAL INFORMATION	12
16. PUBLICATION OF INFORMATION	12
17. USE OF CCTV	13
18. ACADEMIC RESEARCH	13
19. ABUSE OF PRIVILEGES AND NON COMPLIANCE	14
20. ADVERSE INCIDENT REPORTING	14
21. CONFIDENTIALITY AUDITS	15
22. CONSULTATION, APPROVAL AND RATIFICATION PROCESS	15
23. REVIEW AND REVISION ARRANGEMENTS	15
24. DISSEMINATION AND IMPLEMENTATION	15
25. DOCUMENT CONTROL INCLUDING ARCHIVING ARRANGEMENTS	16
26. MONITORING COMPLIANCE WITH AND THE EFFECTIVENESS OF PROCEDURAL DOCUMENTS	16
27. REFERENCES	18
APPENDIX 1: CALDICOTT PRINCIPLES	19
APPENDIX 2: COMMON LAW DUTY OF CONFIDENTIALITY	20

1. Introduction

- 1.1. The North East Ambulance Trust (NEAS) is committed to a policy of protecting the rights and privacy of individuals (includes patients, staff and others) in accordance with the Data Protection Act, hereafter referred to as the 'Act'. The Trust needs to process certain information about its staff, patients and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, monitor performance and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.
- 1.2. This policy aims to detail how NEAS meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the policy are primarily based on the Act and is the key legislation covering security and confidentiality of personal information.
- 1.3. The Act legislates for the protection of personal information relating to living individuals. The Access to Health Records Act 1990 will remain relevant for information relating to deceased persons.
- 1.4. The nature of the work undertaken by the Trust's employees, volunteers and contractors brings them into possession of a great deal of confidential, and often highly sensitive information, both patient and non-patient related. Therefore, it is essential that the public at large have confidence that the organisation as a whole maintains confidentiality of information in whatever form it is given, to whoever it is given and for whatever purpose.

2. Purpose

- 2.1. The purpose of this policy is to ensure the protection of NEAS's information in accordance with the Act. The principle behind this policy is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trusts security systems or controls in order to do so.
- 2.2. The NHS has in place requirements for the handling of confidential patient identifiable information, that were outlined in the Caldicott Report of 1997, the recommendations of which were subsequently implemented within all NHS organisations and are known as the Caldicott Principles.
- 2.3. Caldicott operates alongside and in addition to specific guidance and requirements of professional codes of conduct, such as the NHS Confidentiality Code of Practice.

3. Scope

- 3.1. This policy covers all sites and systems operating and utilised by NEAS. It includes both computer and manual based systems.
- 3.2. The policy applies to any individual employed, in any capacity, by the Trust.
- 3.3. Any breach of the Act or the Trust Data Protection Policy is considered to be an offence and in that event, NEAS disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Trust, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments / sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

4. Definitions

- 4.1. **Data controller** is any person (or organisation) who determined the purposes for which and the manner in which any personal data are, or are to be processed.
- 4.2. **Data subject** is any living individual who is the subject of personal data held by an organisation.
- 4.3. **Personal data** is data which relate to an individual who can be identified from those data or from those data and other information which is in the possession of, or likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any person in respect of the individual. Personal information includes name, address, date of birth, or any other unique identifier such as NHS Number, hospital number, national insurance number etc. It also includes information which, when presented in combination, may identify an individual e.g. postcode etc.
- 4.4. **Processing** is any operation related to organisation, retrieval, disclosure and deletion of data and includes:
 - Obtaining and recording data;
 - Accessing, altering, adding to, merging, deleting data;
 - Retrieval, consultation or use of data and
 - Disclosure or otherwise making available of data.
- 4.5. **Relevant filing system** is any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "relevant filing system" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

- 4.6. **Sensitive personal data** is defined in Section 2 of the Act as data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. These data are subject to more stringent conditions on their processing when compared to personal information.
- 4.7. **Third party** is any individual / organisation other than the data subject, the data controller (Trust) or its agents.

5. Responsibility and Accountability

- 5.1. Overall responsibility for the confidentiality and security of patient and staff information lies with the Chief Executive. Implementation of and compliance with the policy is delegated to the Caldicott Guardian for patient information and Director of Human Resources for staff information. The Trust as a body corporate is the data controller.
- 5.2. **The Data Protection Lead** is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for members of the Trust.
- 5.3. **The NEAS Information Governance Working Group (IGWG)** is responsible for providing advice on data protection issues and to provide support for the Data Protection Lead. This group is also responsible for developing, maintaining and implementing the Data Protection Policy and procedures across NEAS ensuring that they meet national and legislative requirements in relation to Act.
- 5.4. **Senior Managers, Heads of Departments / Sections** and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the Trust.
- 5.5. Compliance with data protection legislation is the responsibility of all members of the Trust who process personal information and include contractors, temporary staff and students. Members of the Trust are responsible for ensuring that any personal data supplied to the Trust are accurate and up-to-date.
- 5.6. Notification is the responsibility of the Chief Executive and the Data Protection Lead. Details of the Trust's notification are published on the Information Commissioner's website. Anyone who is, or intends, processing data for purposes not included in the Trust's Notification should seek advice from the Data Protection Lead.

6. Equality and Diversity Statement

- 6.1. The Trust is committed to providing equality of opportunity, not only in its employment practices but also in the services for which it is responsible. As such, this document has been screened, and if necessary an EIA has been carried out on this document, to identify any potential discriminatory impact.

6.2. If relevant, recommendations from the assessment have been incorporated into the document and have been considered by the approving committee. The Trust also values and respects the diversity of its employees and the communities it serves. In applying this policy, the Trust will have due regard for the need to:

- Eliminate unlawful discrimination.
- Promote equality of opportunity.
- Provide for good relations between people of diverse groups.
- For further information on this, please contact the Equality and Diversity Department.

7. Legal and Professional Obligations

7.1. The disclosure of confidential information needs to be both lawful and ethical. There is a range of legislation and guidance that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range that require information to be used or disclosed.

- Data Protection Act 1998
- Access to Health Records 1990
- Freedom of Information Act 2000
- Human rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- The Telecommunications Regulations 2000
- Obscene Publications Act 1959 and 1964 amendments
- Copyright, Design and Patents Act 1988
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976 and subsequent amendments
- Computer Misuse Act 1990
- Disability Discrimination Act 1995

8. Data Protection Act 1998

8.1. The key statutory requirement for NHS compliance with confidentiality is the Act. This Act legislates for the processing of the personal information of living individuals. The term 'processing' includes any action performed on the data including obtaining, holding, recording, using and disclosing. The Act applies to staff as well as patient records and covers both paper and electronic records.

- 8.2. The long title for the Act is “An act to make new provision for the regulation for the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.”
- 8.3. Any individual has the right to see what information is held about them, and may challenge this information if they feel it is inaccurate or has caused damage to them. The Act places obligations on those who record and use information about individuals. They must register the use of that information (through the Information Commissioner) and they must ensure that they follow sound practices in recording and using the information, in line with the Data Protection Principles.

9. Data Protection Principles

9.1. The Act is based around 8 principles, all of which must be adhered to, to maintain compliance. NEAS fully endorses and adheres to these principles.

9.2. The 8 Data Protection principles are:

9.2.1. **Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.**

There should be no surprises, so inform data subjects why you are collecting their information, what you are going to do with it and who you may share it with, e.g.

- When formulating a research project remember to be open and transparent about what you will be doing with the information.
- When working in a team, ensure that the patient / client is aware of who the members of the team are, and that all those involved with their care may need to see their notes.

9.2.2. **Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.**

- Personal information on e.g. Cleric must only be used for healthcare purposes - not for looking up friends' addresses.
- Only share information outside your team, department or service if you are certain it is appropriate and necessary to do so.

9.2.3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.**

- Only collect and keep the information you require. It is not acceptable to hold information unless you have a view as to how it will be used.
- Do not collect information “just in case it might be useful one day!” e.g. taking both daytime and evening telephone numbers if you know you will only call in the day.
- Explain all abbreviations.
- Use clear legible writing.

- Stick to the facts - avoid personal opinions and comments.

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

- Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the Trust are accurate and up-to-date.
- Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the Trust of any changes in circumstance to enable personal records to be updated accordingly.
- It is the responsibility of the Trust to ensure that any notification regarding change of circumstances is noted and acted upon.
- Check existing records thoroughly before creating new records and avoid creating duplicate records.

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

- Follow retention and disposal guidelines as per the Trusts policy.
- Ensure regular housekeeping / spring cleaning of your information.
- Do not keep “just in case it might be useful one day!”.
- Dispose of your information correctly.

9.2.6. Personal data shall be processed in accordance with the rights of the data subject under the Act.

- Subject access.
- Prevent processing for direct marketing.

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

- Ensure security of confidential faxes by using Safe Haven / Secure faxes.
- ALWAYS keep confidential papers locked away.
- Have a clear desk policy.
- Ensure confidential conversations cannot be overheard.
- Keep your password(s) secret.
- Ensure information is transported securely.

9.2.8. Personal data shall not be transferred to a country or a 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.

- Data must not be transferred outside of the European Economic Area (EEA) which includes the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual.
- Members of the Trust should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

10. Information Provided to Data Subjects

- 10.1. The Act requires that information regarding the nature of the information collected and its uses within the Organisation is communicated to the individuals to whom the data relates. This is known as 'Fair Processing' information.
- 10.2. NEAS shall ensure that the following minimum information is communicated to the individuals to whom the data they hold relates:
- The identity of the Data Controller.
 - The identity of the Organisations nominated representatives, usually the Data Protection Lead.
 - The purpose or purposes for which personal information is processed.
 - Potential disclosures of personal information and who information may be disclosed to.
 - Any further information, which is necessary to make the processing fair.

11. Individual Rights

- 11.1. The aim of the Act is to provide a balance between the fundamental rights and freedoms of individuals against the legitimate personal data processing operations in existence within society today. Data Subjects have the following rights regarding data processing, and the data that are recorded about them:
- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
 - To prevent processing likely to cause damage or distress.
 - To prevent processing for purposes of direct marketing.
 - To be informed about mechanics of automated decision taking process that will significantly affect them.
 - To take action to rectify, block, erase or destroy inaccurate data.
 - To seek compensation if they suffer damage by any contravention of the Act.
 - To request the Commissioner to assess whether any provision of the Act has been contravened.

12. Subject Rights

12.1. Rights of access to personal data

12.1.1. Data subjects have the right to access any personal data which are held by the Trust in electronic format and manual records which form part of a relevant filing system. For employees, this includes the right to inspect confidential personal references received by the Trust about that person. Any individual who wishes to exercise this right should apply in writing to the Data Protection Lead / nominated administrator.

12.1.2. The data subject is entitled to be given a description of:

- The personal data of which that individual is the data subject.
- The purpose for which they are being or are to be processed.
- The recipients or classes of recipients to whom they are or may be disclosed.

12.1.3. In order for the request for information to be valid, three specific criteria must be established and the controller does not have to meet his obligation in fulfilling the request until they are met.

- The request must be made in writing (fax, letter or email).
- The request must be accompanied by the appropriate fee (if applicable).
- The data controller must be satisfied as to the identity of the requestor.

12.1.4. Information supplied should be intelligible and any codes or jargon explained. The Trust is not obliged to comply with repeat identical requests made by an individual unless a reasonable time period has passed.

12.2. Requests on behalf of the data subject

12.2.1. Anyone applying for data subject access on behalf of someone else must have the authorisation of the data subject in writing accompanied with the signature of the data subject.

12.2.2. Someone with parental responsibilities, (if a guardian or grandparent or other holds parental responsibility they will need to present the legal evidence) can submit a subject access request on behalf a child however, if the child is at an understandable age (not defined under the Act) then the child must give consent to the person with parental responsibilities for them to access the information on their behalf.

12.2.3. When responding to a request from a father applying for access to their child's record, the law states that if the father was not married to the child's mother at the time of the child's birth that access cannot automatically be given. Consent must be gained from the child if they are of an understandable age or if they are of an age where they do not understand consent must be gained from the child's mother or appointed guardian.

12.2.4. Where a patient is incapable of managing their affairs someone appointed to act on their behalf by a court of law may submit a subject access request. Proof of the court order should be given.

12.2.5. Where a solicitor, lawyer or other legal professional request for access on behalf of a client they are representing, access may be given with the consent of the client. The legal professional must have written and signed consent of their client. The request must be applied for and processed in the same way it would if it came direct from the data subject. However, this may be an early indicator of a potential claim against the Trust and the Risk and Claims Department should be notified.

12.2.6. In some circumstances the Trust may be asked to provide information to other agencies. In any circumstances the data subject should be informed and they should consent to this.

12.2.7. Under the Access to Health Records Act 1990 a request to see a deceased patient's health record can be made by the patient's personal representative or any person who may have a claim arising out of the patient's death. This is the only case where access to the deceased health records can be given and the Access to Health Records act 1990 must be followed.

12.2.8. The Access to Health Records Act 1990 relates to health records manually stored on or after 1 November 1991 and computerised data can be obtained from 1984 onwards.

12.3. Charges and timescales

12.3.1. There are varying charges available for differing types of data which are prescribed and identified in certain secondary legislation and regulations of the Act.

Subject Access type	Maximum fee	Response Period
Records held manually / computerised – within previous 40 days	Free	40 calendar days
Records held manually / computerised – not within previous 40 days	£10	40 calendar days
Credit Reference Agency	£2	7 working days
Educational records	£50	
Health records held totally on computer	£10	40 calendar days
Health records held totally in manual form	£50	40 calendar days
Health records held part manually part computer	£50	40 calendar days

12.3.2. The information should be supplied in a permanent format unless:

- To do so would involve disproportionate effort. (In these circumstances the requester could be invited to the Trust to view the information).
- The individual has agreed otherwise.

12.4. Third party data

12.4.1. The Trust is not obliged to comply with a request if doing so would reveal the identity of another individual, unless:

- The other individual has given their consent.
- It is reasonable to comply without gaining consent.

12.4.2. Access may be denied or restricted if access to all or part of the record will seriously harm the physical or mental well-being of the individual or any other person. If possible the individual should be provided with access to that part of the record that does not pose the risk of serious

harm. When deciding whether to release third party details without consent, consideration should be given to whether:

- There is a duty of confidence to the other individual.
- Appropriate steps have been taken to gain consent.
- The other individual is capable of giving consent.
- The other individual has expressly refused to give consent.

12.5. General principles of disclosure

12.5.1. The Trust must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Trust business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the Trust concerned.

12.5.2. This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

- The individual has given their consent (e.g. a patient / member of staff has consented to the Trust corresponding with a named third party).
- Where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other Trust employees if it is clear that those members of staff require the information to enable them to perform their jobs).
- Where the institution is legally obliged to disclose the data (e.g. equality monitoring).
- Where disclosure of data is required for the performance of a contract (e.g. PCTs / Other Trusts / SHA, DH).

12.5.3. The Act permits certain disclosures without consent and a full list can be found in Confidentiality Policy and Code of Conduct.

12.5.4. As an alternative to disclosing personal data, the Trust may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer.
- Accept a sealed envelope / incoming email message and attempt to forward it to the data subject.

- 12.5.5. Please remember to inform the enquirer that such action will be taken conditionally: i.e. "if the person is a member of the Trust" to avoid confirming their membership of, their presence in or their absence from the institution.
- 12.5.6. If in doubt, staff should seek advice from their Head of Department / Section or the Trust Data Protection Lead.

13. Consent

13.1. General principles

- 13.1.1. Wherever possible, personal or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Trust understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.
- 13.1.2. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.
- 13.1.3. In most instances consent to process personal and sensitive data is obtained routinely by the Trust (e.g. when a new member of staff signs a contract of employment). Any Trust forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.
- 13.1.4. If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.
- 13.1.5. If any member of the Trust is in any doubt about these matters, they should consult the Trust Data Protection Lead.

14. Security of Data

- 14.1. All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.
- 14.2. All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access;
 - In a locked drawer or filing cabinet;
 - If computerised, password protected or
 - Kept on disks which are themselves kept securely.
- 14.3. Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.
- 14.4. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste." Hard drives of redundant PC's should be wiped clean before disposal.
- 14.5. Appropriate precautions must be taken when transporting personal information, both within and outside the organisation, to ensure that it is protected from unauthorised access, loss or destruction. The protection of information is the responsibility of the member of staff who is in possession of the information. Failure to take adequate measures to protect information may lead to disciplinary and or legal action being taken against the individual.
- 14.6. Off-site processing (at home or in other locations outside the Trust) of personal data is strictly prohibited as it presents a potentially greater risk of loss, theft or damage to personal data.

15. Retention and Storage of Confidential Information

- 15.1. Records containing personal information should not be kept longer than necessary and should be stored appropriately. Guidance on retention periods and the storage of records for both patient and staff records is provided by the Records Management Policy and the Information Security Policy.

16. Publication of Information

- 16.1. All members of the Trust should note that the Trust publishes a number of items that include personal data, and will continue to do so. These personal data are:
- Information published on the Trust Internet / Intranet site including:-
 - Names of members of the Trust Board.
 - Internal Telephone Directory.
 - Staff qualifications, long service awards, etc.
 - Videos or other multimedia versions of training exercises and ceremonies.
 - Information in Staff Magazines (including photographs), annual reports, staff newsletters, etc.
 - Staff information on the Trust website (including photographs).

- 16.2. It is recognised that there might be occasions when a member of staff requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the Trust should comply with the request and ensure that appropriate action is taken.
- 16.3. Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (e.g. an opt-out box on a form).

17. Use of CCTV

- 17.1. The Trust's use of CCTV is regulated by a separate Code of Practice.
- 17.2. For reasons of personal security and to protect Trust premises and the property of staff, close circuit television cameras are in operation in Headquarters, in certain station and hospital locations. The presence of these cameras may not be obvious.
- 17.3. This policy determines that personal data obtained during monitoring will be processed as follows:
- Any monitoring will be carried out only by a limited number of specified staff.
 - Personal data obtained during monitoring will be kept for 30 days and destroyed as soon as possible after any investigation is complete.
 - Staff involved in monitoring will maintain confidentiality in respect of personal data.

18. Academic Research

- 18.1. Personal data collected only for the purposes of academic research must be processed in compliance with the Act. Researchers should note that personal data processed ONLY for research purposes receive certain exemptions (detailed below) from the Act if:
- The data are not processed to support measures or decisions with respect to particular individuals AND
 - If any data subjects are not caused substantial harm or distress by the processing of the data.
- 18.2. If the above conditions are met, the following exemptions may be applied to data processed for research purposes only:
- Personal data can be processed for purposes other than that for which they were originally obtained (exemption from Principle 2).
 - Personal data can be held indefinitely (exemption from Principle 5).

- Personal data are exempt from data subject access rights where the data are processed for research purposes and the results are anonymised (exemption from part of Principle 6 relating to access to personal data).
- 18.3. Other than these three exceptions, the Act applies in full. The obligations to obtain consent before using data, to collect only necessary and accurate data, and to hold data securely and confidentially must all still be complied with.
- 18.4. **Notes to researchers**
- 18.4.1. Whilst the Act states that research may legitimately involve processing of personal data beyond the originally stated purposes, the Trust hopes that, wherever possible, researchers will contact participants if it is intended to use data for purposes other than that for which they were originally collected.
- 18.4.2. Although the Act allows personal data processed only for research purposes to be kept indefinitely, researchers are asked to refer to the Trust's Policy on Records Management.
- 18.4.3. For those departments which gather sensitive personal data (as defined by the Act), extra care should be taken to ensure that explicit consent is gained and that data are held securely and confidentially so as to avoid unlawful disclosure.

18.5. **Publication**

- 18.5.1. Researchers should ensure that the results of the research are anonymised when published and that no information is published that would allow individuals to be identified. Results of the research can be published on the web or otherwise sent outside the European Economic Area but if this includes any personal data, the specific consent of the data subject must, wherever possible, be obtained.

19. **Abuse of Privileges and Non Compliance**

- 19.1. It is strictly forbidden for employees to look at any information relating to their own family, friends or acquaintances without consent. Looking at patient or staff records out of curiosity is totally unacceptable. Disciplinary proceedings may be instigated should abuse of privilege be discovered.
- 19.2. All staff agree to uphold confidentiality on signing of their contract of employment with the Trust. This agreement continues after employment has ceased. Non-compliance with this statement and this code of practice may result in disciplinary action being taken in accordance with the NEAS Disciplinary Procedure.

20. **Adverse Incident Reporting**

- 20.1. Possible breaches or risks of breaches of this policy or other confidential information will constitute an adverse incident and will be reported through the Trust incident reporting

procedure. The Trust risk register will be used to log any identified risks to the protection of personal information.

21. Confidentiality Audits

21.1. Electronic information

Audits of access to personal information will be undertaken regularly by the Trust to identify misuse and compliance with this policy. Any incidents of suspected misuse will be fully investigated and may result in disciplinary action.

21.2. Manual information

Each area where personal information is retained must develop and implement procedures for the regular audit of access to that information.

22. Consultation, Approval and Ratification Process

22.1. Consultation

22.1.1. This document has been produced by the author on behalf on the IGWG. This group was consulted upon and their comments added to the document as appropriate.

22.2. Approval and ratification

22.2.1. The Trust Policy Review Group is the committee with the authority for the review of this document. The Joint Consultative Committee and the Trust Board are responsible for ratifying this policy

22.2.2. The IGWG has carried out a full and proper consultation and has considered the content of the document in terms of current best practice, guidelines, legislation and mandatory and statutory requirements, in considering the document for approval the committee also took into account the results of the recommendations of the EIA.

23. Review and Revision Arrangements

23.1. The document will be reviewed at least annually or when appropriate after changes in legislation or guidance. The document owner will be responsible for this review.

24. Dissemination and Implementation

24.1. Dissemination

24.1.1. This policy is available for all staff to access via the Trust Quality System. Staff without computer network access should contact their line manager for information on how to access policies.

24.1.2. All staff will be notified of new or revised documents via internal communications systems.

24.1.3. This document will also be included in the Publication Scheme for NEAS in compliance with the FOI Act 2000.

24.2. Implementation

24.2.1. This policy will be implemented in the following ways:

- Regular communications to staff on new policies and procedures through IG Circulars.
- Regular audit of information governance (IG) processes undertaken in line with policies and procedures in key areas i.e. records management, confidentiality, information security, FOI and data quality.
- Monitoring through the Information Governance Toolkit (IGT).

24.3. Training

24.3.1. Training will be regularly assessed and refreshed in order that staff may remain appropriately skilled / knowledgeable over time.

24.3.2. Broad IG training will be included in the Trust induction programme. Additional training can be requested at the discretion of a manager, or by an individual wanting personal development along with mandatory yearly update training.

24.3.3. Further guidance and information relating to data protection issues will be distributed periodically via various media including the intranet site, 'The Pulse' (monthly service journal) and via email.

25. Document Control Including Archiving Arrangements

25.1. Register / library of procedural documents

All documents shall be held within the Trust Quality System and will be managed in line with quality standards.

25.2. Archiving arrangement

Archiving of documents will be in line with the Records Management Policy.

26. Monitoring Compliance With and the Effectiveness of Procedural Documents

26.1. Process for monitoring compliance

26.1.1. All staff must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for data protection.

26.1.2. Failure to follow this policy and related IG policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member.

26.1.3. Monitoring staff compliance through:

- Verifying that, where appropriate, agreement to disclosure decisions are recorded.
- Obtaining patient feedback of the process, e.g.:

- Did they understand when and to whom their information would be disclosed?
- Did they understand the choices available to them regarding disclosure?
- Did they have the opportunity to ask questions and have them answered?
- Did they understand that withholding of consent does not affect the way they are handled by staff but may reduce the number of treatment options available to them?
- Did they feel under pressure to agree to disclosure?
- Evaluating whether staff understand disclosure issues and their responsibility for obtaining consent.
- Evaluate how staff handled questions about disclosure, and in particular review cases where:
 - Patients have declined to agree to disclosure.
 - Patients have changed their disclosure decision during the care episode.
 - A senior healthcare professional has overridden a non-disclosure decision

26.2. Standards and Key Performance Indicators

There are a number of national standards and requirements relating to IG.

26.2.1. IG Toolkit

The connecting for Health IGT is a framework for implementing the IG agenda and consists of a series of requirements against which an organisation's current and planned attainment levels can be monitored. The Trust is required to complete a self assessment by 31st March each year, the results which will contribute to the assessment undertaken by the Healthcare Commission.

26.2.2. Standards for Better Healthcare

- The Department of Health's standards for better health include 24 core standards that all NHS healthcare providers in England should achieve, and 13 developmental standards that they should be working towards achieving.
- Core standard 13 requires that health care organisations have systems in place to ensure that:
 - Staff treat patients, their relatives and carers with dignity and respect;
 - Appropriate consent is obtained when required for all contracts with patients and for the use of any patient confidential information; and
 - Staff treat patient information confidentially, except where authorised by legislation to the contrary.

26.2.3. NHS Litigation Authority

- The NHSLA Risk Management Standard for Ambulance Trusts applies to all Ambulance Trusts are designed to address organisational, clinical, and non-clinical / health and safety risks.

- Parts of the Clinical Care standard are of relevance to IG, including patient / service user identification and quality of written and electronic clinical records.

27. References

- Department of Health NHS IG Guidance on Legal and Professional Obligations.
- NHS Connecting for Health IG Toolkit <https://www.igt.connectingforhealth.nhs.uk/>

Appendix 1: Caldicott Principles

The Caldicott Principles were introduced by the 1997 check date Caldicott Report into the uses of patient-identifiable information within the NHS. The principles it devised are to ensure that access to and use of personal information is restricted to justifiable purposes and to authorised staff.

The Caldicott Principles are:

1. Justify the purpose(s).
2. Don't use patient identifiable information unless it is absolutely necessary.
3. Use the minimum amount of patient identifiable information.
4. Access to patient-identifiable information should be on a strict need to know basis.
5. Everyone should be aware of his or her responsibilities.
6. Understand and comply with the law.

Caldicott also requires the establishment of Information Sharing Protocols to govern the sharing or patient information between partner organisations. This is to ensure that each organisation receiving information will handle and protect that information in a similar way.

Appendix 2: Common Law Duty of Confidentiality

Personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information. This duty of confidence is long established in common law.

The Department of Health's guidance to the NHS is that, with proper safeguards, the duty of confidence need not be construed so rigidly that, when applied to NHS or related services, there is a risk of it operating to the disadvantage of a patient or to the public generally.