North East Ambulance Service NHS
NHS Foundation Trust

Confidentiality Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-1
Version Number	02
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance & Resources
Ratifying Committee	Finance Committee
Date Ratified	18 February 2016
Date Policy Effective From	18 February 2016
Next Review Date	18 February 2019
Keywords	Anonymised information; Clinical audit; Confidential information; Disclosure; Explicit; express consent; Healthcare purposes; Implied consent; Information sharing protocols; Medical purposes; Personal data; Public interest; Sensitive personal data.

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
01	1.2 2.10 6.1 6.3, 6.4, 6.5 10.3.1 11.4.1 6.5.1 16.6	• Section expanded. • Removal of Health & Social Care Act 2001. • Updated. • Amended to personal information. • Expanded. • 4th bullet removed. • Expanded. • Updated.	R Oliver	Nov 2013
02	All	• Full review and transfer onto new template. • Consistent application of the term 'confidential'. • Addition of new section relating to staff information. • Updated Caldicott Principles. • Updated reference to policies. • Compliance and Risk Committee replaced with Finance Committee as ratifying group.	R Oliver	Dec 2015
02	6.9.7	• General statement added for release of information to professional bodies. • Document renamed Confidentiality Policy	R Oliver	Jan 2016

This page should not be longer than one single page.

Table of Contents

1. Introduction 5
2. Purpose 5
3. Scope 5
4. Duties - Roles & Responsibilities 6
   - 4.1 Chief Executive 6
   - 4.2 The NEAS Information Governance Working Group (IGWG) 6
   - 4.3 All staff 6
5. Glossary of Terms 6
6. Policy Content 8
   - 6.1 Legal and Professional Obligations 8
   - 6.2 Protecting Information 11
   - 6.3 Confidentiality Clauses 12
   - 6.4 Subject Access Requests 12
   - 6.5 Confidentiality of Patient Information 13
   - 6.6 Disclosure of Patient Information 14
   - 6.7 Patient Choice 16
   - 6.8 Confidentiality of Staff Information 17
   - 6.9 Specific Departmental Considerations 22
   - 6.10 Confidentiality Audits 24
   - 6.11 Abuse of Privileges and Non Compliance 24
   - 6.12 Adverse Incident Reporting 24
7. Training Required for Compliance with this Policy 24
8. Equality and Diversity 24
9. Monitoring Compliance with and Effectiveness of this Policy 25
   - 9.1 Compliance and Effectiveness Monitoring 25
   - 9.2 Compliance and Effectiveness Monitoring Table for this policy 26

10. Consultation and Review of this Policy 27

11. Implementation of this Policy 27

12. References 27

13. Associated Documentation 27

1. Introduction

This policy has been developed in line with the national NHS Code of Practice on Confidentiality and describes the responsibilities of all staff and lays down guidelines in order to ensure confidentiality is maintained.

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, staff and Trust related. Therefore, it is essential that the public at large believe 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. The Trust also has statutory obligations to maintain records, systems and procedures ensuring they are stored and disposed of accordingly.

All staff working for the North East Ambulance Service NHS Foundation Trust (NEAS) have a legal duty of confidentiality to the subjects of information they come into contact with. This duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence (e.g. patient to healthcare professional).

2. Purpose

The purpose of this document is to outline the organisation's intentions and approach to fulfilling its statutory and organisational responsibilities around confidentiality.

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.

3. Scope

This policy should be adhered to by all staff employed by the Trust and / or with a responsibility for Trust data, which may include contractors, volunteers or staff employed by other organisations but working on behalf of the Trust.

This policy covers all aspects of information within the Trust including but not limited to:

- Patient / client / service user information
- Staff information
- Corporate information

Any breach of the NHS Code of Practice on Confidentiality or the Trust Confidentiality 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 confidential 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. Duties - Roles & Responsibilities

4.1 Chief Executive

Overall responsibility for the confidentiality and security of patient, staff and corporate 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 Strategy, Transformation and Workforce for staff information.

4.2 The NEAS Information Governance Working Group (IGWG)

Developing, maintaining, implementing and monitoring this policy and associated procedures across NEAS ensuring that they meet national and legislative requirements in relation to confidentiality.

4.3 All staff

All staff within North East Ambulance Service NHS Foundation Trust are responsible for ensuring that the principles outlined within this policy are universally applied.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Anonymised information	Information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.
Clinical audit	The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services. This should be distinguished from studies that aim to derive, scientifically confirm and publish generalised knowledge. The first is an essential component of modern healthcare provision, whilst the latter is research

Term	Description
	and is not encompassed within the definition of clinical audit in this document.
Confidential information	Any information held, both personal and non-personal, that when provided was done so in the expectation it would not be disclosed without relevant authority. It can be anything that relates to patients, staff, their family and friends and also to Trust information that is protected from release under the Freedom of Information Act 2000 (FOI). Confidential information includes but is not limited to: • Personal details of any patient. • Information pertaining to diagnosis, prognosis or treatment where this is linked to an identifiable individual. • Information contained within the personnel records of any employee. This class of information may be stored in any manner e.g. on paper, electronically, video, photograph, and could be stored on any device, including portable such as laptops, mobile phones, palmtops and digital cameras. Confidential information may also be passed by word of mouth
Disclosure	Divulging or provision of access to data.
Explicit or express consent	Means articulated agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.
Healthcare purposes	Include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.
Implied consent	Agreement that has been signalled by behaviour of an informed individual.

Term	Description
Information sharing protocols	Documented rules and procedures for the disclosure and use of personal information, which specifically relate to security, confidentiality and data destruction, between two or more organisations or agencies.
Medical purposes	Include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services.
Personal data	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.
Public interest	Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.
Sensitive personal data	Defined in Section 2 of the Data Protection Act 1998 (DPA) 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.

6. Policy Content

6.1 Legal and Professional Obligations

The duty of confidentiality arises out of the common law of confidentiality,

professional obligations, and also staff employment contracts (including those for contractors). 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.

6.1.1 Data Protection Act 1998

The key statutory requirement for NHS compliance with confidentiality is the DPA. 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.

NEAS meets its obligations under the Act as it works in line with the 8 Data Protection principles:

- Data shall be processed fairly and lawfully.
- Data shall be processed only for specified purposes.
- Data shall be adequate, relevant and not excessive.
- Data shall be accurate and kept up to date.
- Data shall not be kept for longer than necessary.
- Data shall be processed in accordance with individual's rights.
- Data shall be kept secure.
- Data shall not be transferred outside the European Economic Area (EEA) without adequate protection.

The Act allows for third party access to personal information in certain specified circumstances, known as exemptions. Further information can be found on the Information Commissioner's website – https://ico.org.uk/.

6.1.2 Freedom of Information Act 2000

This Act came into full effect on the 1st January 2005 and legislates from the general right of access to non-personal information held by public authorities. The idea behind this Act was to encourage greater openness by these authorities.

The Act contains a number of exemptions – valid reasons – why a request for information can be refused. Further information can be found on the Information Commissioner's website – https://ico.org.uk/.

6.1.3 Human rights Act 1998

Article 8 of the Human Rights Act 1998 establishes a right to 'respect for private and family life'. This identifies a duty to protect the privacy of individuals and preserve

the confidentiality of their health records. Compliance with the DPA ensures the Trust is meeting its obligations under Human Rights legislation.

6.1.4 Common Law of Confidentiality

This is not written in statute but is based on legal precedent. Any personal information given or received in confidence for one purpose may not be used for a different purpose or disclosed without the consent of the provider of the information. Two exceptions to the common law duty exist where information may be disclosed without consent, these are:

- Where there is an overriding public interest in the disclosure, for example where there is a significant risk to the safety of one of more individuals.
- Where the disclosure is required by law or requested by the court.

6.1.5 Caldicott Principles 1997

The original Caldicott Report, published in 1997, established six principles for NHS bodies (and parties contracting with such bodies) to adhere to in order to protect patient information and confidentiality.

The government commissioned Dame Fiona Caldicott to conduct a further Information Governance Review (the “Review”) which was published at the end of April 2013. There are now 7 Caldicott Principles:

- Justify the purpose.
- Only use person identifiable information when absolutely necessary.
- Use the minimum necessary personal confidential data.
- Access to personal confidential data should be on a strict need to know basis.
- Everyone with access to personal confidential data should be aware of their responsibilities.
- Comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

6.1.6 Crime and Disorder Act 1998

The Crime & Disorder Act provides the power to disclose information to the Police for the purposes of preventing or detecting crime. It does not provide a duty to disclose, and does not override a healthcare professional’s common law duty of confidence.

6.1.7 Computer Misuse Act 1990

The Computer Misuse Act makes it an offence to access information held within a computer system without authority. Staff therefore must only access information that

they are authorised to access, must not provide access to computer systems to others (by allowing others to use their password) and staff must not alter information where they are not authorised to do so.

The Computer Misuse Act creates three specific offences:

- Unauthorised access to computer material.
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a crime.
- Unauthorised modification of computer material.

6.2 Protecting Information

All staff have a duty to protect the information they handle on a day-to-day basis. Just because systems or circumstances may allow you access to certain information this does not mean that you have a legitimate reason to view or disclose it.

6.2.1 Recording information accurately and consistently

Maintaining proper records is vital to patient care and staff records. If records are inaccurate, future decisions may be wrong and harm an individual. If information is recorded inconsistently, then records are harder to interpret, resulting in delays and possible errors. The information may be needed not only for the immediate treatment of the patient and the audit of that care, but also to support future research that can lead to better treatments in the future.

The practical value of privacy enhancing measures and anonymisation techniques will be undermined if the information they are designed to safeguard is unreliable.

6.2.2 Keeping personal information private

This includes aspects such as:

- Not gossiping – this is clearly an improper use of confidential information.
- Taking care when discussing cases in public places - it may be pertinent to discuss cases with colleagues for professional reasons (to gain advice, or share experience and knowledge), but care must be taken to ensure that others do not overhear these conversations. Generally, there is no need to identify the individual concerned.

6.2.3 Keeping personal information physically and electronically secure

Portable computers or paper files should not be left in unattended cars or in easily accessible areas. Ideally, store all files and portable equipment under lock and key when not actually being used.

Records should not be taken home, and where this cannot be avoided, procedures for safeguarding the information effectively should be agreed via the Caldicott Guardian or Director of Strategy, Transformation and Workforce for staff information.

Do not leave confidential information on view. Paper files should be locked away in drawers / cabinets. Staff should 'log out' of computers when not at their desk.

- Never share your password with anyone else.
- Confidential phone calls should not be conducted in an open office.
- Adopt a 'clear desk policy'.
- Do not disclose confidential information over the telephone unless you are 100% certain of the identity of the caller. If in doubt, check the caller's identity and establish whether they are in fact entitled to receive the information. Call back if necessary. If in doubt, do not release the information and check with the Information Governance Manager.
- Faxing confidential information should only be used if the receiving fax is classified as a safe haven fax. Ask the recipient to confirm receipt of the fax as soon as it is received. Reference should be made to Transfer of Personal Information Policy.
- Patient identifiable and personal information should not be sent unencrypted via email as its security cannot be assured.

Trust information must not be removed from the Trust premises without appropriate and documented authorisation. Electronic information must not be transferred to or stored on any removable storage device (such as a USB memory stick, CD or DVD etc.) without explicit authority to do so from the Trust Caldicott Guardian and/or Director of Strategy, Transformation and Workforce.

Further information can be found in Information Security Policy, Transfer of Information Policy and Records Management Policy.

6.3 Confidentiality Clauses

Staff contracts - All staff contracts, whether permanent, temporary or agency, must contain a suitable confidentiality clause which outlines the employees responsibilities. Breaches of confidentiality may be viewed as gross misconduct under NEAS Code of Conduct, and could result in termination of employment.

Professional Codes of Conduct - In addition to clauses contained within staff contracts and terms and conditions, staff also have obligations in relation to confidentiality that are identified within their professional codes of conduct. All staff must ensure that they are fully aware of these and abide by their requirements.

6.4 Subject Access Requests

Requests by individuals to access their own records, both staff and patient, are known as 'Subject Access Requests' and are a given right under the DPA. All requests must be made in writing and completed within 21 days. Reference should be made to the Data Protection Policy when handling these requests. It is not always necessary to complete a Trust request form if there is sufficient information provided

by the data subject in their written request.

6.5 Confidentiality of Patient Information

6.5.1 General principles

The confidentiality of patient information must be safeguarded, particularly where this information is shared between the NHS and its partner organisations. However it is essential that confidentiality does not act as a barrier to the provision of care. There are many situations where the exchange of patient identifiable information is necessary for the efficient and effective operation of the Trust and its partner organisations. The aim is to ensure that information remains accessible to those who need to know, whilst ensuring that the information is adequately protected from unauthorised access and that where appropriate patients are fully aware of who their information is disclosed to and why.

Staff are only authorised to access information that is relevant to their role, where they are involved directly with the care of individual patients. Staff must not deliberately access their own clinical records, either manual or electronic, or the records of relatives or friends unless this is done through a formal Data Protection access request. Staff may only access the records of friends or relatives where this is required as part of their job role at that time.

6.5.2 Information relating to minors

Children and young people are entitled to the same duty of confidentiality as adults – providing that those aged under 16 are judged by professionals to understand their choices and the potential outcomes of sharing information (known as Gillick competence). Parental consent should be sought to share information about a child or young person (in law, those under the age of 18).

Exceptions to this are when contact with an individual or individuals who have 'Parental Responsibility' would be more likely than not to jeopardise the safety or welfare of the child / young person; or, doing so would conflict with the wishes of the child / young person. Gillick competence means that "…the parental right to determine whether or not their minor child below the age of 16 will have medical treatment terminates if and when the child achieves sufficient understanding and intelligence to enable him to understand fully what is proposed." Lord Fraser, Gillick v West Norfolk Area Health Authority 1985.

The Data Protection (Subject Access Modification)(Health) Order 2000 provides that; where information has been provided by a child in the expectation that it would not be disclosed to their parent / guardian, or where it has been obtained as a result of any investigation to which the child consented in the expectation that it would not be disclosed, or where the child has expressly indicated that the information should not be disclosed, parent / guardians have no automatic right of access where a child has been deemed Fraser competent and is aged 12 or over.

6.5.3 Patient Consent

Where information about patients is required, but does not satisfy the tests of necessity and appropriateness that must govern the use of identifiable patient

information, then it should be anonymised to protect the patient.

In all other circumstances efforts must be made to obtain and record consent unless there are statutory grounds for setting confidentiality aside or robust public interest issues. Whilst it is necessary to disclose information about a patient to those staff who are providing or auditing care, it is important to ensure that those who see information have a genuine need to know.

6.6 Disclosure of Patient Information

6.6.1 General principles

Staff must ensure that patients within their care are kept fully informed of the purposes for which information about them is collected and those to whom this information may be disclosed. Specifically, patients have the right to make decisions as to whether or not information about them is disclosed either in relation to healthcare provision or for non-healthcare care purposes. The disclosure of information for healthcare purposes is not normally an issue for the great majority of patients, however where appropriate patients must be given opportunities to raise objections and concerns.

6.6.2 Sharing information outside the NHS

Sharing with partner organisations outside the NHS must be based on either consent or a statutory requirement. Where not required by legislation, information sharing must be covered by an appropriate Information Sharing Protocol or contract.

6.6.3 Requests from the Police

Requests are often received from the police for copies of patient report forms, incident logs and tapes of calls and other personal information. The Police do not have an automatic right of access to information held by the Trust. Where a request is received, certain information can be released without consent if there is a legal justification for disclosure.

Where the information is required to assist the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty, Section 29 of the DPA can be applied. This section does not ‘require’ the disclosure of information; it merely provides the Trust with a legal basis under which it may release the information.

However, these requests must be made in writing using the official police form (these will differ from force to force) or NEAS 137 Police Request for Personal Data form.

Under no circumstances should information be handed out at the scene of an incident. All requests are logged by Clinical Audit and the Control Room Manager.

6.6.4 Requests for non-personal information

Requests for non-personal information are governed by the requirements of the FOI Act. Reference should be made to Freedom of Information Policy prior to releasing information.

6.6.5 Requests from the media

Under no circumstance should personal or non-personal information be given out to the media. If you receive a request from the media by personal visit, phone, email or post, please forward and refer that person to the Trust PR Department.

6.6.6 Requests from solicitors

A letter of authorisation must accompany requests from solicitors for information pertaining to their client from the individual who is the subject of the information. These are handled by the Clinical Care and Patient Safety Directorate.

6.6.7 Requests for information from other individuals

Requests for information from other individuals, whether they be patients or staff should only be released on a 'need to know' basis. The requester must be able to justify why the request is being made and that they are entitled to make the request.

There are circumstances when information can be released to third parties. Further guidance can be found in the Data Protection Policy.

6.6.8 Telephone enquiries

If a request for information is made over the telephone, the response will be dependent on who is making the request, and what the request is for:

- Never release any confidential information over the telephone unless you are entirely sure of the identity of the caller and their entitlement to receive the information. If in doubt, call them back. Further guidance can be found in the Transfer of Personal Information Policy.

- Individuals making a request for their own personal information must be asked to put their request in writing (email is acceptable).

- An individual making a request under FOI must be asked to put their request in writing (email is acceptable).

6.6.9 Requests from overseas

There may be occasions when confidential information is requested from overseas or must be transferred overseas when accompanying a foreign national who may have received treatment from NEAS. Although these will be rare occurrences, procedures must be followed to protect the information. The 8th Data Protection Principle states:

'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'

The Act makes allowances for the transfer of medical information to accompany a patient. Ideally, when transferring personal information outside of the EEA, consent

should be obtained from the data subject. However, if this is not possible, the following conditions must be satisfied prior to its release:

- The reason for the information request is valid.
- The method of transferring the information is secure.
- Details on how the information will be kept secure by the recipient are supplied and
- There is a documented retention period for the information.

Only when these conditions are satisfied should the information be released.

6.7 Patient Choice

It is essential for patients to be informed, in ways they can understand, of the purposes for which information about them is collected and how their information will be shared.

Patients should be advised how information will be used at the time they are asked to provide it, and should have the opportunity to discuss any aspects that are special to their treatment or circumstances.

6.7.1 Information leaflets

Advice about the use of patient information will be made available through the use of newsletters, leaflets and posters displayed in appropriate areas. In particular, the Trusts leaflet Patient Information and Confidentiality should be used for this purpose.

Advice and information must be presented to patients in a convenient and understandable form. It should be available both for general purposes and before a particular programme of care or treatment begins.

Where patient identifiable information is being used in ways that do not directly contribute to, or support the delivery of their care, patients should be informed of this and the patient's decision to restrict the disclosure of their information is appropriately respected.

6.7.2 Informing patients

To ensure we inform patients correctly, the following guidelines should be followed:

- Make clear to patients when information is or may be disclosed to others - staff must ensure that patients know when data is disclosed or used more widely.
- Check that patients are aware of the choices available in respect of how their information may be used or shared.
- Check that patients have no concerns or queries about how their information is used.

- Respect the right of patients to have access to their health records – through access to health records and Data Protection Policy.
- Communicate effectively with patients to help them understand.
- Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of their care.
- Respect patients' decisions to restrict the disclosure and / or use of information.
- Explain the implications of disclosing and not disclosing.

6.8 Confidentiality of Staff Information

Confidential information may be passed on to someone else:

- with the subject's consent or
- on a strictly controlled 'need to know' basis.

6.8.1 Need to know basis

For NHS purposes (including where services are either provided under contract to the NHS or are being planned or provided with other agencies), including, but not limited to:

- Recruitment.
- Personnel Management matters (this includes, but is not limited to, for absence management, payroll, pension etc.).
- Reports for Department of Health.

6.8.2 Wider purposes

- Assuring and improving the quality of patient care and treatment (clinical audit).
- Monitoring and protecting public health.
- Effective health care administration such as:
    - Managing / planning services.
    - Contracting for NHS services.
    - Auditing NHS accounts and accounting for NHS performance.
    - Risk management (health and safety).
    - To investigate complaints.

  - For statistical analysis, and for medical or health services research.

- The information is required by statute or Court Order.
- The passing on of information for safeguarding.
- Police, coroner and other official requests for information under the Crime and Disorder Act.

6.8.3 Sharing staff information

Staff will be requested to provide personal information for purposes such as for recruitment processes, medical assessments or personal development/staff management purposes.

The processes for sharing staff information can be divided into 3 different areas:

- Where subject consent is NOT REQUIRED.
- Where subject consent is IMPLIED.
- Where explicit subject consent is REQUIRED.

6.8.4 Where subject consent is NOT REQUIRED

Trust employment law solicitors

From time to time it may be necessary for the Trust to contact solicitors to request guidance and advice on employment law issues. This may not require the disclosure of staff details and the individual in question will remain anonymous.

Where a solicitor is acting on behalf of the Trust for example, in relation to an Employment Tribunal or other legal claim, employee details may be provided without consent.

Solicitors engaged will be responsible for the confidentiality of any information provided to them by Trust.

Contracted out services

There may be some services which the Trust contracts out to 3rd Parties. Where possible, the Trust will only provide the information which is relevant. There are some instances (e.g.: Payroll) where 3rd parties can directly access electronic data held on staff on Trust databases and will do so in order to provide services to the Trust. In all cases of 3rd party involvement, the 3rd party will be bound by a contractual agreements.

NHS/Department of Health (DOH) purposes

The Trust will be required to provide information on its staff to appropriate official bodies to facilitate statistical analysis, resource planning and healthcare management.

The Department of Health requires an annual workforce report, and adhoc requests are received from various other NHS related organisations. Where anonymised data is not suitable, identifiable data may be provided as long as the request is for legitimate purposes.

Protection of the public

Passing on information to the appropriate authorities to help prevent, detect or prosecute serious crime or dangers to the general public, such as public health risk or risk of violence, may be justified to protect the public. Although there is no absolute definition of serious crime, section 116 of the Police and Criminal Evidence Act 1984 identifies some serious arrestable offences, which include:

- Treason
- Murder
- Manslaughter
- Rape
- Kidnapping
- Certain sexual offences
- Causing an explosion
- Certain firearm offences
- Taking of hostages
- Hijacking
- Causing death by reckless driving

There are also offences under the prevention of terrorism legislation and also making a threat which if carried out would be likely to lead to:

- Serious threat to the security of the state or to public order.
- Serious interference with the administration of justice or with the investigation of an offence.
- Death or serious injury.
- Substantial financial gain or serious financial loss to any person.

Directors and Department Heads may need to seek advice before taking a decision to release information.

Police enquiries

Information may be provided to the Police for the purposes of investigating a crime. The request must be made in writing by the relevant Police Officers on a Data Protection Form which they must submit to Trust. (Section 29 – Disclosure of Information)

It is important that this form should be signed by an officer at an appropriate level. Where the subject of the enquiry is under investigation, they should not be informed in case this would affect the progress of the investigation.

Court orders

Where a Court Order is received requesting the disclosure of employee information, this must be provided. E.g.: CSA enquiries, proceedings for personal injury or death. The subject of the enquiry will not be told of the request.

Counter Fraud

The Trust may provide details to the appropriate authorities, either pro-actively or on request to facilitate counter fraud investigations where an anomaly has been identified. The subject of the enquiry should not be made aware of the investigation.

Statutory requirements

The majority of statutory requirements concern forms of notification to the appropriate authorities: for example, communicable diseases, substance misuse (Misuse of Drugs Act 1971, s.10 and Misuse of Drugs (Supply to Addicts) Regulations 1997 and serious accidents (in particular under the Health and Safety at Work etc. Act 1974).

6.8.5 Where subject consent is IMPLIED.

Human resource functions

It is understood by employees that their details will be used for appropriate purposes within the Human Resource function and for day to day resource management and these functions are considered to be understood and accepted by the provision of the required information. This includes:

- Payroll
- Personnel database
- Personnel files
- Pensions
- Sickness absence
- Shift rotas
- General management within the Trust.

- Disclosure and Barring Service (DBS) check

Certain staff members will be subject to a DBS check due to their position within the Trust. This is conducted in accordance with the DBS Policy. Individuals will receive a letter explaining the requirements of the process and a form to be completed. Completion of this form implies that the individual consents to the process.

Pre-employment references

Applicants complete a standard application form which requests the nomination of referees and asks whether the referees may be contacted before an offer of employment is made. The intention to contact these referees is given and therefore the provision of referee details is accepted as consent for these referees to be contacted for this purpose.

Employment references for existing employees

When an existing employee applies for alternative employment they may provide the new potential employer with details of their current employer for reference purposes. Where the Trust is approached by a potential new employer, consent for the Trust to provide the required information is implied by the fact that the employee has provided the potential new employer with appropriate contact details.

Occupational Health

The standard Trust employment contract may require staff to undergo medical examination by a registered medical practitioner nominated by the Trust, should it be deemed necessary to assess medical fitness during the course of their employment.

By signing the contract an employee accepts the terms and conditions outlined within the contract and therefore consents to medical examination. This implies consent for the necessary personal information to be provided to Occupational Health personnel and for appropriate advice and information to be shared with the Trust by Occupational Health.

Occupational Health maintain their own medical records relating to Trust personnel and are responsible for ensuring the confidentiality of all information they hold.

When it is deemed necessary for an employee to be referred to Occupational Health during the course of their employment, this will be discussed with the individual in question before a referral is made.

Training/education

External training companies will be provided with the necessary information relating to members of staff undertaking training courses with them. Only the required information will be provided. The member of staff in question will either have requested the training themselves, or have agreed to undertaking it, and this would therefore imply consent for this information to be provided

There may be occasions where the Trust agree to support training when an employee is first offered a position (e.g.: C1 driver training). Again the completion by

the employee/potential employee of the relevant paperwork implies consent for provision of the necessary information.

6.8.6 Where explicit subject consent is REQUIRED

Non-Employment References

There may be occasions where financial institutes, rental agencies etc. will contact the Trust to enquire about the employment status and remuneration of an employee. Express written consent from the employee is required before any information is released.

Occupational Health

Where it is considered appropriate for an employee to be referred to an outside agency under occupational health such as physiotherapy, the individual's Manager will discuss this with them and obtain their consent before any referral is made. Employees will be made aware of the implications of declining a referral.

Counselling

Where it may be appropriate for an employee to receive counselling, following a traumatic incident for example, the employee will be provided with the appropriate contact details and will contact the service themselves. Referrals may be made by a line manager or Human Resources but only following discussion with and consent from the individual.

Medical Records

Where Occupational Health hold medical records on Trust staff, accepted medical record responsibilities will apply and the subject must provide written consent to the Occupational Health body before they release any medical information to any third party requestor.

Trade Unions

Trade Union representatives may request employee information on behalf of one of their members in relation to a grievance or dispute. The staff representative will be pursuing the case at the request of the employee and consent of the employee is required. Only information relating to that particular employee should be provided.

External Requestors

All other parties requesting information relating to members of staff must provide the written consent of the individual in question e.g.: Solicitors acting on behalf of the employee, family members etc.

6.9 Specific Departmental Considerations

All staff need to be aware of the confidential nature of information they handle as part of their role. In addition there are specific considerations for certain areas of the Trust.

6.9.1 Operational staff

Operational staff are the employees who will have the most direct contact with patients and their relatives. Information confided during treatment and / or transportation, whether this is by word of mouth or held in writing, must be kept confidential in accordance with this policy.

On occasions, staff may be required to provide statements to the police with reference to incidents they may have attended. This is acceptable if the police have completed the necessary paperwork (see Police Requests).

Operational staff may be required to obtain evidence of clinical experience to complete their portfolios, in the form of PRFs. If this is the case, staff members must request the information from the Clinical Care & Patient Safety Directorate who will ensure that all patient identifiable details have been anoymised and do not appear in the photocopied document.

6.9.2 Control staff

Control staff who have contact with patients and their relatives on a day-to–day basis must respect the confidentiality of these individuals at all times. In addition, due to the nature of the functions carried out in the control room, it is also necessary to store information pertaining to operational staff on the CAD system. This information must be handled with the utmost confidentiality.

6.9.3 Human Resources and Occupational Health

Personnel records and staff occupational health records afford the same level of protection as patient information, as laid down in this policy and staff should respect the privacy of other staff members at all times.

6.9.4 IM&T Staff

IM&T staff will have access to databases and applications that process personal information and privacy of such information should be respected**.** During the course of such access, personal and/or confidential data may be processed by staff and this will regarded as a professional privilege. There may not be any further use of this information outside the normal performance of the staff duties.

6.9.5 Clinical Care & Patient Safety Staff

Clinical staff have access to all the patient report forms completed by the operational staff throughout the Trust. They will also have access to incidents and litigation documents which all contain a substantial amount of sensitive personal and patient information, these must be treated in accordance with the requirements of this policy.

6.9.6 PALS and Complaints Staff

Information handled by the PALS and Complaints staff may contain particularly sensitive information relating to both staff and patients. The confidentiality of this must be maintained at all times. Any disciplinary proceedings brought as a result of a complaint will also be kept strictly confidential.

6.9.7 Professional bodies

NEAS will cooperate with the release of any information to professional bodies as part of their internal investigations in line with professional practice and any other regulatory provision

6.10 Confidentiality Audits

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

6.11 Abuse of Privileges and Non Compliance

Breach of confidence, inappropriate use of personal records or abuse of computer systems may lead to disciplinary measures, bring into question professional registration and possibly result in legal proceedings. 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.

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 may result in disciplinary action being taken in accordance with the Disciplinary Policy.

6.12 Adverse Incident Reporting

Possible breaches or risks of breaches of 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 confidentiality of information.

7. Training Required for Compliance with this Policy

All staff will receive annual information governance training through the Trust Training Department which will include confidently.

8. Equality and Diversity

The Trust is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on the grounds of any protected characteristic (Equality Act 2010). An equality analysis has been undertaken for this policy, in accordance with the Equality Act (2010).

An equality analysis has been undertaken for this policy, in accordance with the

internal Equality Policy and the Equality Act (2010).

Details of this assessment are stored within the central register for Equality Analysis Assessments maintained within the Equality and Diversity team within the Communications and Engagement department.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	Monitoring and audit					
	Key Performance Indicators (KPI)/ Criteria	**Method**	**Who By**	**Committee**	**Frequency**	**Learning/ Action Plan**
Adverse confidentiality related incidents.	Number of confidentiality incidents by: • Type (patient/staff) • Department • Severity	Report from Trust incident reporting system.	Risk Management Support Officer.	Information Governance Working Group.	Bi-monthly.	• Additional training to staff. • Further audit of department concerned.

10. Consultation and Review of this Policy

This policy has been reviewed in consultation with the Information Governance Working Group and Trust Directors.

11. Implementation of this Policy

This policy will be implemented in the following ways:

- Inclusion in the Trust “Summary”.
- Q-Pulse alert.

12. References

- NHS Code of Practice on Confidentiality
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human rights Act 1998
- Common Law of Confidentiality
- Caldicott Principles 1998
- Crime and Disorder Act 1998
- Computer Misuse Act 1990

13. Associated Documentation

This policy refers to the following Trust documents:

- Transfer of Information Policy
- Information Security Policy
- Records Management Policy
- Data Protection Policy
- Freedom of Information Policy

- DBS Policy
- Disciplinary Policy
- Equality Policy