REF: IG 08

VERSION: 6.0

North Cumbria University Hospitals NHS Trust

Data Protection Policy

SUMMARY & AIM

This Policy details how the Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the policy are primarily based upon the Data Protection Act 1998, which is the key piece of legislation covering security and confidentiality of personal information.

This Policy provides the employees of North Cumbria University Hospitals NHS Trust with a comprehensive framework through which all personal identifiable data is acquired, stored, processed and transferred in accordance with the Data Protection Act 1998 and the Caldicott Principles.

TARGET AUDIENCE:

All employees, temporary / contract staff / data processor personnel who process personal data on behalf of the Trust will comply with this Policy.

TRAINING:

Information Governance annual training includes Data Protection compliance

EVIDENCE OF IMPLEMENTATION:

- Annual update of the Trust's Data Protection Notification to the Information Commissioner's Office
- Subject Access Request compliance reports to the Information Governance Group
- Mandatory training completion rates reported at Workforce Group

KEY REQUIREMENTS

1. Consistent compliance with the requirements of the Data Protection Act 1998 when processing personal identifiable information

2. The appropriate creation; storage; retention; accuracy; relevance; disclosure and disposal of personal data

DOCUMENT CONTROL

Author/Contact	Tracey Best – Information Governance Manager & Anne Gadsden – Governance Information Officer Tel: 01228 602186 Email: tracey.best@ncuh.nhs.uk Anne.gadsden@ncuh.nhs.uk
Executive Director	Director of Finance
Equality Impact Assessment Date	13/04/2016
Version	6.0
Publication Date	03/05/2016
Review Date	31/05/2019
Sub-Committee & Approval Date	Information Governance Group – 12/02/2016
Date ratified by Trust Policy Group	21/04/2016
Date noted by Safety & Quality Committee	14/06/2016
Policy Reference	IG 08
Please note that the Intranet version of this document is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.	

History of previous published versions of this document:

Date Approved by Sub Committee	Date Ratified by TPG	Version	Issue Date	Review Date	Policy Author Details
02/12/2013	10/01/2014	5.0	19/02/2014	21/12/2015	Deputy Director IM&T
09/09/2011	06/12/2011	4.0	21/12/2011	31/12/2013	Deputy Director IM&T
20/11/2008	08/12/2008	3.0	01/2009	07/04/2011	Information Governance Officer
12/06/2007	30/05/2007	2.0	26/06/2007	26/06/2009	Information Governance Officer
		1.0	01/2003		

Statement of changes made from version 5.0

Version	Date	Section & Description
5.1	12/01/2016	Policy update to include key elements of 'buddy' Trust Northumbria's Data Protection Policy (DPP) • Sections 1, 2.2, 2.3, 2.4, 3.1, 4.2, 4.5, 4.7, 6.2.1, and 6.2.2 amended to reflect Northumbria's DPP • Amendment to Director of Governance job title (Section 4.3) • Addition of Section 4.8 (Information Governance Officer Responsibilities) • Completion of Section 8 (Process for monitoring compliance) • Completion of Policy 'top sheet'
5.2	16/02/2016	• Highlights taken out of document, Summary section removed (already on front page of document) and subsequent sections renumbered
5.3	21/04/2016	Amendments following Trust Policy Group meeting 21/04/2016: • Addition of Flowchart, and re-numbering of subsequent sections • Addition of Section 4.11 Human Resources Team responsibilities for processing staff information Subject Access Requests. Renumbering subsequent sub-sections • Add reference to Section 6.2 and 6.3 in Section 2.1

List of Stakeholders who have reviewed the document

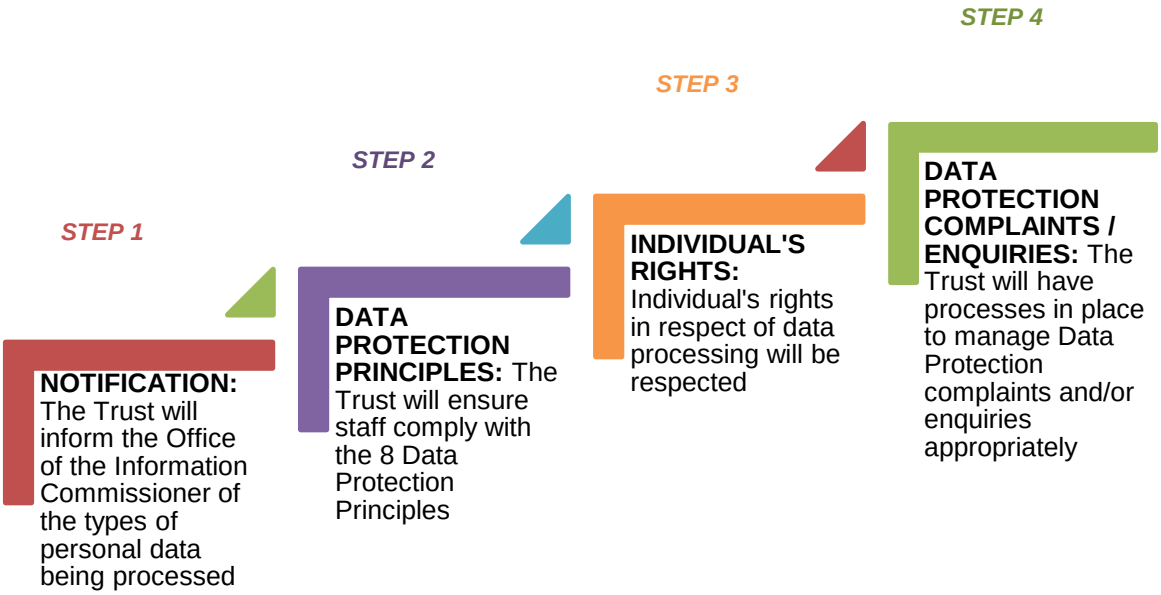
(*list should include anyone or department head of departments with responsibilities)*

Name	Job Title	Date
Graham Putnam	Caldicott Guardian	13/01/2016
Dave Tomlinson	Director of Finance / Senior Information Risk Owner (SIRO)	13/01/2016
Derrick Bates	Trust Information Security Officer (TISO)	13/01/2016
Michelle Woodward	Interim Associate Director of Risk and Governance	13/01/2016
	Business Unit Directors	13/01/2016

TABLE OF CONTENTS

1. SUMMARY FLOWCHART:

Data Protection Act 1998



2. INTRODUCTION

2.1 The Data Protection Act 1998 ('the Act') gives effect in UK law to European Commission Directive 95/46/EC, and introduces Eight Data Protection Principles that set out standards of information handling. These standards apply to all data controllers who process personal data. The Trust, as a Public Authority, is a Data Controller.

Essentially the Act does three things:

1. It requires every data controller to inform the relevant national authority of its processing operations ('Notification')
2. It obliges data controllers to comply with a code of conduct on data processing (the 'Data Protection Principles' – see section 6.2);
3. It creates a set of enforceable expectations for individuals concerning the processing of their personal data (the 'Individuals' Rights' – see section 6.3).

2.2 The Trust is required by law to comply with the Data Protection Act 1998. It is the commitment of the Trust to ensure that every employee complies with this Act to ensure the confidentiality of any personal data processed by the Trust in whatever medium (i.e. electronic systems, manual filing system).

2.3 All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the Trust. This relates to roles that are reliant upon computer systems such as: patient administration, purchasing, invoicing and treatment planning. Recent legislation also regulates the use of manual records relating to patients, staff and others whose information may be held within the Trust.

2.4 The Trust needs to collect and use certain types of information about people with whom it deals in order to operate. These include current past and prospective patients/service users and employees, suppliers and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 1998.

3. PURPOSE

3.1 This Policy has been developed to provide guidance, assistance and awareness for Trust staff to ensure a standard, consistent compliance to processing (creation; storage; retention; accuracy; relevance; disclosure and disposal) of personal identifiable data.

4. DUTIES (ROLES & RESPONSIBILITIES)

4.1 CEO / Trust Board Responsibilities

The Chief Executive is responsible as Accounting Officer for ensuring that the Trust is legally compliant with the Data Protection Act 1998.

4.2 Director of Finance Responsibilities (Senior Information Risk Owner)

The Director of Finance as Senior Information Risk Owner acts as an advocate for information risk on the Trust Board. In addition they provide written advice to the accounting officer on the content of the annual statement of internal control in regards to information risk.

4.3 Associate Director of Risk and Governance Responsibilities

The Associate Director of Risk & Governance will receive and process complaints about non supply of information considered to be exempted and the application of the Trust's procedures.

4.4 Information System (Asset) Owners (IAO) Responsibilities

The Trust is the data controller. However, it is the responsibility of any person creating a new computer or manual filing system, which will be used by other employees, to ensure that the eight Data Protection principles have been followed (see Section 6.2). The Trust's Data Protection Officer must also be informed before a new or upgraded system is put in place. Privacy Impact Assessments will be applied as required.

4.5 Caldicott Guardian Responsibilities

The Caldicott Guardian has a strategic role which involves representing and championing confidentiality and information sharing requirements and issues at senior management level. In addition they actively support information sharing and advise on options for lawful and ethical processing of information.

The Caldicott Guardian is also responsible for assuring the Trust Board that Data Protection Policies and systems complying with the Data Protection Act are in place, and that a suitably trained and experienced Data Protection Officer is identified and notified to the Information Commissioner's Office.

4.6 Data Protection Officer's Responsibilities

The Data Protection Officer for the Trust is responsible for:

- Providing expert advice in respect of the Data Protection Act to the Trust Board and its senior officers.

- Ensure that the access and informed consent provisions of the Data Protection Act are met by means of procedures applied by Subject Access Coordinators, systems, training and publicity.
- Ensuring that there are processes in place for risk assessment, compliance audits and reports to the Information Governance Group in respect of Data Protection issues.

On a day-to-day basis the Data Protection Officer will in addition be responsible for the following:

- Ensuring that appropriate Data Protection Act notification is maintained for applicable organisation's systems and information.
- Dealing with enquires, from any source, in relation to the Data Protection Act; facilitating Data Subject Notices.
- Advising users of information systems, applications and networks on their responsibilities under the Data Protection Act, including Subject Access.
- Investigating or Reviewing Incident Reports in respect of possible breaches of the Act and agreeing the recommended actions as part of the Trust and Health Service and Social Care Information Centre Serious Incident Procedures
- Encouraging, monitoring and checking compliance with the Data Protection Act.
- Liaising with external organisations on Data Protection Act matters.
- Promoting awareness and providing guidance and advice on the Data Protection Act as it applies within the organisation, and generally ensuring that the Trust fulfils its role as Data Controller.
- Ensure that there are processes in place to respond to the 6th Data Protection principle (see 6.2.6 below) and S.10 notices from Data Subjects

4.7 Information Governance Manager Responsibilities

The Information Governance Manager is responsible for the following

- Acting as initial point of contact for any data protection issues which may arise within the Trust;
- Publicise and Promote this Policy;
- Ensuring training programme is in place to support the policy;
- Maintaining Data Protection registration;
- Monitoring performance of this policy through Quality Control and Internal Audits.

4.8 Information Governance Officer (IGO) Responsibilities

The Information Governance Officer has day-to-day responsibility for ensuring the Subject Access Coordinator processes are implemented, and to ensure that their procedures are updated and maintained to reflect current working practices.

The Information Governance Officer will provide quarterly reports to the Information Governance Group (IGG) with information on the number of

information requests made, completed application forms returned and requests completed. The report will also include details of compliance with the 40-day response target.

4.9 Deputy Business Unit Director Responsibilities

Deputy Business Unit Directors and their equivalent in respect of Corporate Services are responsible for ensuring that all staff within their Business Unit are aware of the Data Protection Policy and apply the principles of the Act.

4.10 Subject Access Coordinators Responsibilities

Subject Access Coordinators are employed to process Subject Access Requests for patient health records. They will follow detailed procedures, referring any issues which require further direction to the Information Governance Officer.

4.11 Human Resources Team Responsibilities

Members of the Human Resources team will process Subject Access Requests for staff information. They will follow detailed procedures, referring any issues which require further direction to the Information Governance Officer.

4.12 Information Governance Group Responsibilities

The Information Governance Group will review the application of this policy and receive exception reports in respect of compliance from the Data Protection Officer in its capacity as a delegated authority of the IM & T Group.

4.13 Line Managers Responsibilities

Line Managers (General Managers, Operational Service Managers or equivalent Heads of Department in Corporate Services) are directly responsible for:

- Reading this policy and ensuring that all permanent and temporary employees in their remit comply with the Data Protection Act 1998.
- Ensuring the security of the organisation's information assets, that is information, hardware and software used by staff and, where appropriate, by third parties, is consistent with legal and management requirements and obligations.
- Ensuring that their staff conform to system level security policies and system operating procedures as defined in the Information Risk Policy.
- Ensuring that their staff are aware of their security and confidentiality responsibilities.
- Ensuring that their staff have had suitable security and mandated Information Governance training.
- Ensure that staff are specifically aware of the powers of the Information Commissioner in respect of serious contraventions of the Act in respect of Data Loss and the duty of the Trust to report such incidents through the NHS and Social care Information Centre

4.14 Staff Responsibilities

All Trust Staff and contractors acting for the Trust have a statutory duty of confidentiality to protect personally identifiable (patient and staff) information and only use it for the purposes for which it was intended.

All staff and contractors have a duty to:

- Conform to system level security policies and system operating procedures as defined in the Information Risk Policy.
- Be aware of their security responsibilities.
- Attend suitable security and mandated Information Governance training.
- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the organisation's IT systems.
- Report on any suspected or actual breaches in security.
- Generally to comply with the 8 Data Protection Principles (see Section 6.2 below)
- Comply with the Caldicott Principles (appendix 1)

Breach of confidentiality is a serious matter that may result in disciplinary action by the Trust or the appropriate professional regulatory body, or legal action by a patient.

5. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
DPA	Data Protection Act 1998
CEO	Chief Executive Officer
HSCIC	Health and Social Care Information Centre
IAO	Information Asset Owner
ICO	the Office of the Information Commissioner, the regulatory Authority
IGO	Information Governance Officer
NCUHT	North Cumbria University Hospitals NHS Trust
NHS	National Health Service
SAC	Subject Access Coordinator
SIRO	Senior Information Risk Owner

TERM USED	DEFINITION
Data Controller	any person (in the legal sense) who controls the processing of personal data.
Data Processor	any person who processes data on behalf of the Data Controller
Data Subject	the individual person who is the subject of any relevant personal data.
Health and Social Care Information Centre	the body responsible for incident investigation and reporting within the NHS in England through which ICO may be notified.

TERM USED	DEFINITION
Information Asset Owners	Senior members of staff who take responsibility for Information Assets such as information systems - further defined in the Trust's Information Risk Policy.
Personal Data	electronic or manual information which identifies a living individual
Processing	any activity that can be carried out concerning personal data.
Sensitive Personal Data	information as to a person's religious beliefs or beliefs of a similar nature, racial or ethnic origin, membership of a trade union, political opinions, physical or mental health, sexual life or criminal record.
S.10(of the Data Protection Act) Notice	Intimation by a Data Subject that processing by a Data Controller results in damage or distress and to which a response must be made within 21 days
S.30 (of the Data Protection Act) Notice	Enables a regulation permitting the lead health professional to advise the Data Controller that release of information to a data subject could damage their health or that of a third party
The Act	Data Protection Act 1998

6. POLICY:

The Trust will handle personal data in accordance with the Act by:

- Obtaining and processing personal data in such a way that recognises the conditions for fair processing, for compliance with a legal obligation to which the Trust is subject, and for the exercise of the Trust's statutory functions;
- Collecting and processing personal data on a 'need to know' basis, ensuring that it is fit for purpose, not excessive, is disposed of at a time appropriate for its purpose and that adequate steps are taken to ensure the accuracy and currency of data;
- Ensuring that for all personal data, appropriate technical and organisational measures are taken to prevent damage, loss or abuse;
- Ensuring that the movement of personal data is done in a lawful way – both inside and outside the organisation;
- Acknowledging the rights of individuals to whom the personal data relates and ensure that these rights may be exercised in accordance with the Act.
- Ensuring that the Information Commissioner is notified of all relevant processing and will conduct a periodic review and update of the register entries to ensure that they remain up to date;
- Ensuring that an active 'fair processing' framework is in place, through which patients and staff are informed about the kind of purposes for which information about them is collected, and the categories of people or organisation to which such personal information may be passed. Such a framework will ensure that an individual's consent to the use of their information is informed.

6.1 Notification

The Trust (through its Data Protection Officer) will inform the Office of the Information Commissioner of the types of processing it undertakes.

The Trust will provide:

- A description of Personal data being processed, and of the categories of data subject to which they relate;
- A description of the purposes for which the data are being / are to be processed;
- The source(s) from which the Trust intends to obtain the information
- A description of all recipients to whom the Trust intends or may disclose information to;
- Details of any processing outside the European Economic Area when the processes underpinning the 8th principle apply (see 6.2 below).

Processing without notification, and processing of a type not reflected in the notification, are both criminal offences. It is also a criminal offence for any Trust employee to knowingly or recklessly operate outside the descriptions contained in the Trust's notification entry

6.2 Data Protection Principles

There are eight principles of data processing:

First Principle	Personal data shall be processed fairly and lawfully
Second Principle	Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes
Third Principle	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
Fourth Principle	Personal data shall be accurate and, where necessary, kept up to date
Fifth Principle	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
Sixth Principle	Personal data shall be processed in accordance with the rights of data subjects under the act
Seventh Principle	Appropriate technical and organisational measure shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
Eighth Principle	Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subject in relation to the processing of personal data

Where third party employees have legitimately and contractually agreed access to the Trust's information systems compliance will be the same as that required in respect of NCUHT employed staff. In the event of confidence being breached by a Third Party contractor, the penalty will be termination of contract, and this will be specified.

These principles are enforceable by the Information Commissioner by virtue of his powers to issue Enforcement Notices. Failure to comply with such an enforcement notice constitutes a criminal offence.

There are various exemptions from the need to comply with the principles. Examples include processing for national security, the prevention or detection of crime, the assessment or collection of tax, the determination of examination results and for the purposes of management forecasting.

6.2.1 Principle 1: Fair and lawful processing

The first data protection principle requires personal data to be processed fairly and lawfully.

The Trust has an obligation to make the general public aware of why the Trust needs information about them, how this is used and to whom it may be disclosed

In many cases the Trust can process personal data only with the implied consent of the individual. In some cases if the data is sensitive express consent must be obtained. Further guidance on obtaining consent can be found in the NHS Confidentiality: NHS Code of Practice and the Trust's Confidentiality Code of Conduct

6.2.2 Principle 2: Obtained for specific purpose

To comply with the second principle the Trust will notify the Information Commissioner's Office (ICO) of all the purposes for which it processes personal data. If the reasons for processing this information are changed, both the ICO and data subjects will be informed.

If the Trust fails to complete this process (and keep the information up to date) it has committed a criminal offence and could face criminal prosecution.

6.2.3 Principle 3: Adequate, relevant, not excessive

Information is collected for specific purposes. The Trust will ensure that the information it collects is not excessive in relation to those purposes, and that it is adequate and relevant enough to carry out the required function.

6.2.4 Principle 4: Accurate and up-to-date

Where the Trust obtains information either directly from the data subject or via a third party, it will ensure the accuracy of the data. If the data subject informs the Trust of a (factual) inaccuracy, the data will be amended to reflect this, if this is agreed. Exceptionally a note will be appended to the record to indicate that the data subject does not agree that the data held is accurate.

6.2.5 Principle 5: Disposal

The Trust will not retain information for longer than it is required to fulfil the purposes for which it is collected. The Trust's retention schedules will be used to ensure that it complies with this principle.

6.2.6 Principle 6: Data subject rights

The data subject has the right to request any information processed by the Trust relating to them. They also have the right to request their personal data be rectified, blocked or erased. It is the responsibility of all staff in the Trust to be aware of the data subject's rights and to respond appropriately to such requests.

(see also section 6.3: Individuals' rights)

6.2.7 Principle 7: Security

The seventh data protection principle requires that all data processing be undertaken in a secure environment. The Trust will take a risk-based approach to security and will take appropriate measures to ensure that unauthorised processing does not occur and that data are not accidentally lost, stolen or destroyed.

6.2.8 Principle 8: Processing outside the European Economic Area

The eighth principle outlaws the sending of personal data to destinations that are not within the European Economic Area. The exceptions to this rule include those countries that have adequate data protection legislation and where consent to the export has been obtained from the data subject, or when a process compliant with guidance issued by the Information Commissioner's Office is in place.

6.3 Individual's rights

Individuals are entitled to the following rights in respect of data processing:

- To be informed by any data controller whether it is processing data concerning him/her, and to be given a copy of such data;
- To prevent processing likely to cause him/her damage or distress;
- To prevent direct marketing to him/her;
- To prevent the taking of automated decisions concerning him/her;
- To have inaccurate data corrected or erased;

- To compensation for damage or distress caused by unlawful data processing; and
- To ask the Information Commissioner to investigate the activities of any data controller.

In respect of data processing for healthcare, the rights of informed consent are modified by the provisions of Section 30 of the Act and also by regulations issued under Section 251 of the NHS Act 2006.

The Trust will endeavour to ensure that where Personal data are being processed by, or on behalf of the Trust, individuals will be given:

- A description of the data;
- Purpose the data is being used for;
- The recipients to whom the data will be disclosed.

6.3.1 Subject Access

Subject access will be managed in line with the rights given to each individual by the Data Protection Act 1998 subject to i) below and other applicable exemptions Access will be provided through application to the Subject Access desk in respect of patients and third parties, the Director of Human Resources in respect of staff or the Data Protection Officer.

The Trust will ensure:

a) All requests for subject access will be accepted in writing only;
b) All requests will be responded to within 40 days from receipt of a valid request or, if later, within 40 days of receipt of –
   - Information confirming identity / legitimacy of individual making the request / assisting in the location of relevant data
   - The fee
c) All requests for subject access will incur a fixed fee up to the maximum permitted within the Act
d) A request will not be met in the absence of:
   - Written request;
   - The fee;
   - Information confirming identity of the individual making the request / assisting in the location of data (where necessary)
e) All requests for subject access will receive a reply even when data is not held about the individual concerned.
f) Where Personal data has been requested, and its release is not covered by exemptions under the Act, a copy of the data held will be supplied to the requester;
g) In the event of information in the copy being unintelligible a reasonable explanation will be given to the requester by an appropriate Trust employee;
h) Where a subject access request has been met previously, additional requests for similar or identical access by the same person will only be met following a reasonable time lapse. In deciding a reasonable time lapse the following factors will be considered:
   - The nature of the data;

- The purpose for which the data are processed;
- Frequency with which the data are altered.

i) Where a subject access request would result in the disclosure of information relating to an individual other than the data subject the Trust will only comply with the request if:
   - The other individual has consented to disclosure of the information;
   - It is reasonable in all the circumstances to comply with the request without the consent of the other individual. In deciding reasonableness the Trust will give regard to:
     - Any duty of confidentiality owed to the other individual;
     - Steps taken to seek the consent of the other individual;
     - Capability of the other individual to give consent;
     - Refusal of consent by the other individual.

j) When requests are made by or on behalf of children, the Trust will at all times work within the law relating to the legal capacity of children (i.e. the request must be in the interests of the child and not just the parents).

k) Requests in respect of patients will be subject to Lead Health Professional assessment of the possible application of S.30

Subject access requests will be referred to the Data Protection Officer if the application of an exemption is being considered.

6.3.2 Data Subject Notices

Under the Act, data subjects have the right to send a notice to the Trust, asking the Trust (within a reasonable time) to stop processing their information. This is a 'data subject notice.'

The Trust will ensure:

a) All data subject notices will be accepted in writing only;

b) A valid notice will include –
   - Identification details of the data subject and a description of the personal data to which they refer;
   - The nature of the processing and whether it is the processing for a specified purpose or in a specified manner to which they object;
   - When the data subject requires the processing of the personal data to cease (this must be at the end of a period which is reasonable in all the circumstances), or that the data subject does not wish the Trust to begin processing their personal data;
   - That the processing of personal data for the purpose specified is causing or is likely to cause the data subject or another persona substantial damage or substantial distress, and that damage or distress would be unwarranted; and
   - The reason why the data subject believes that the processing is causing or is likely to cause them or another person unwarranted damage and/or distress.

c) A data subject notice will not be met in the absence of this information;

d) All data subject notices will be responded to within 28 days from receipt of a valid notice. The response will inform the data subject either

- that the Trust has complied with or intends to comply with the data subject notice; or
- the extent to which the Trust intends to comply, explain which parts of the notice are considered to be unjustified, and why.

Data subject notices will be facilitated by the Trust's Data Protection Officer, who will report on notices and their outcomes through the Trust's assurance processes.

6.4 Data Protection complaints and/or enquiries

Complaints about the Trust's Data Protection procedures, and appeals against decisions not to supply exempt information, will be dealt with by the Director of Governance, who will deal with the complaint in accordance with the Trust's Complaints Policy and Procedure.

General enquiries about the Data Protection Act will be dealt with through the Data Protection Officer.

DPA Section 10 notices from data subjects in respect of the right to prevent processing likely to cause damage or distress will be addressed and responded to by the Data Protection Officer

7. TRAINING AND SUPPORT

Basic awareness training in respect of Data Protection is included within the Trust's induction programme and is reinforced by mandatory annual Information Governance training through the Trust's Information Governance Workbook or e-learning. This meets the requirements of part 2 of the annual Data Protection Notification renewal.

8. PROCESS FOR MONITORING COMPLIANCE

The Trust assesses its compliance with the Data Protection Act by means of the Annual Information Governance submission process and as part of the annual ICO notification renewal process.

The process for monitoring compliance with the effectiveness of this policy is as follows:

Monitoring/audit arrangements	Methodology	Reporting		
		Presented by	Committee	Frequency
Submission against IG Toolkit	Compliance and exceptions report	Information Governance Officer	Information Governance Group	Annual
Subject Access Request compliance report	Compliance and exceptions report	Information Governance Officer	Information Governance Group	Quarterly
Completion of Information Governance mandatory training	ESR report detailing training completion statistics	Learning & Development Lead	Workforce Group	Monthly

Wherever the above monitoring has identified deficiencies, the following will be in place:

- Action plan
- Progress of action plan monitored by the Information Governance Group minutes
- Risks will be considered for inclusion in the appropriate risk registers

9. REFERENCES

Confidentiality: NHS Code of Practice
http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf

[Supplemented by: A guide to confidentiality in health and social care V1.1 September 2013 (Health and Social Care Information Centre)]

Records Management: NHS Code of Practice
http://www.dh.gov.uk/assetRoot/04/13/31/96/04133196.pdf

Data Protection Act 1998 http://www.opsi.gov.uk/acts/acts1998/80029--a.htm

[Amended by S.144 Criminal Justice and Immigration Act 2008 in respect of monetary penalties for serious contraventions mainly of data loss.]

European Commission Directive 95/46/EC
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

National Health Service Act 2006 S.251
http://www.legislation.gov.uk/ukpga/2006/41/section/251

Information Governance Toolkit Requirements (Health and Social Care Information Centre - revised annually): https://nww.igt.hscic.gov.uk/

10. ASSOCIATED DOCUMENTATION

NCAH Confidentiality Code of Practice (Isms 1028)
http://nww.staffweb.cumbria.nhs.uk/acute/policies/a_c/confidentiality%20cop.pdf

Trust Retention Schedules

Medical Records Department: Information Request Procedure (Isms 3010)
http://nww.staffweb.cumbria.nhs.uk/acute/policies/m_s/med%20records%20info%20request.pdf

Policy for Disclosing Information to the Police (Isms 4007)
http://nww.staffweb.cumbria.nhs.uk/acute/policies/d_g/disclosing_information to_police.pdf

Information Security Incident: Reporting and Investigating Procedure
http://nww.staffweb.cumbria.nhs.uk/acute/policies/h_l/informa`tion_security_reporting_procedure.pdf

Information Risk Policy
Information Risk Policy

APPENDIX 1: CALDICOTT PRINCIPLES (REVISED 2013)

- Justify the purpose

  Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian

- Don't use personal data unless it is absolutely necessary

  Personal Confidential data items should not be included unless it is essential for the specified purpose of that flow. The need for patients to be identified should be considered at every stage of satisfying the purpose(s).

- Use the minimum necessary personal confidential data

  Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or is accessible as is necessary for a given function to be carried out

- Access to personal confidential data should be on a 'need to know' basis.

  Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes

- Everyone with access to personal confidential data should be aware of their responsibilities.

  Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality

- Comply with the law

  Every use of personal confidential data must be lawful. Someone in each organisation handling personal data should be responsible for ensuring that the organisation complies with legal requirements

- The duty to share information can be as important as the duty to protect patient confidentiality

  Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

APPENDIX 2 - POLICY SIGNATURE RECORD

Line managers - Print this sheet and record the names of all staff members you are responsible for, who must read and sign they have understood this policy.

POLICY TITLE: Data Protection Policy

By signing this document, I acknowledge I have read the above named policy.			
Name (Please Print)	**Job Title**	**Date**	**Signature**