York Teaching Hospital NHS
NHS Foundation Trust

DATA PROTECTION POLICY

Author:	Susan Hall
Owner:	Elizabeth McManus
Publisher:	Healthcare Governance Directorate
Date of first issue:	September 2004
Version:	4.0
Date of version issue:	April 2013
Approved by:	Executive Board
Date approved:	March 2013
Review date:	July 2017
Target audience:	All Staff
Relevant Regulations and Standards	Data Protection Act 1998, NHS Information Governance standards

Executive Summary
This policy describes how the Trust will meet its obligations under the Data Protection Act 1998. In particular, it sets out the actions required to comply with the eight enforceable principles of quality and security, which must be observed when handling information about living individuals, be they patients, staff, volunteers or others in contact with the Trust.

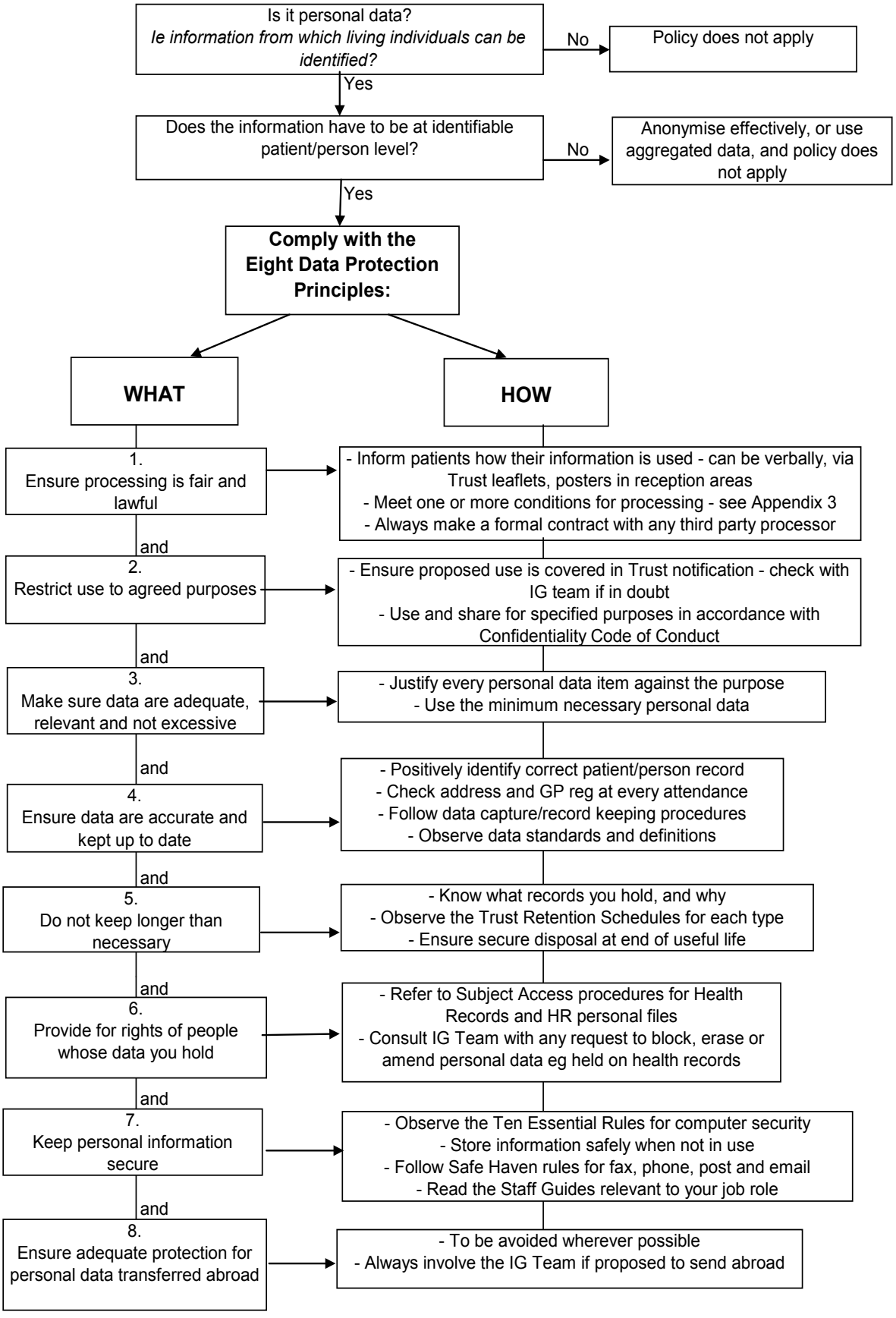
VERSION HISTORY LOG

Version	Date Approved	Significant Changes
1.0	December 2004	New Policy.
2.0	September 2007 Agreed Fiona Jamieson	No new requirements. Conformed to current Trust policy template and revised review date. Otherwise minor changes to post and organisation titles, updated document references etc.
3.0	October 2009 Agreed Fiona Jamieson	No new requirements under DPA but policy updated to reflect changes in penalties for breaches of the Act, and extended Information Governance requirements in respect of security incident management. Otherwise minor changes to post and organisation titles, updated document references etc.
3.1	November 2011	Addition of Caldicott, SIRO and Clinical IT Lead roles. Changes to titles of posts and committees. Updated references to standards and guidance. Introduced definitions of Safe Havens and Information Risk Management. Inserted link to Trust's notification (removed summary at Appendix 5) Full policy review scheduled for November 2012
4.0	October 2012	Policy revised following acquisition of Scarborough. Conformance to most recent Policy Template. Changes to titles of posts and committees. Updates to standards and legislation. Addition of Privacy Impact Assessments, new mandatory training requirements and IG training needs assessment.
	July 2017	Extended until July 2017 to incorporate new GDPR

Author for all versions: Susan Hall, Information Governance Lead Manager
Location: Staff Room (Trust Intranet), under Corporate Policies and Procedures

Contents

Policy Flowchart



1. Introduction and Scope

1.1 The Data Protection Act 1998 ("The Act") is the key piece of privacy legislation in the UK. The Act seeks to find a balance between the often competing interests of individual rights to privacy, and the need for organisations to carry out their legitimate functions. Data Protection is of special importance in the realm of health care, where much ***sensitive personal information**** is in routine use.

1.2 The Act works in two ways:

a) It places obligations on those who process ***personal information***, so that quality and security are maintained

b) it gives rights to individual ***data subjects***, granting them a degree of control over how their information is used.

1.3 Data Protection is a risk issue for the Trust. Any failure to comply with the Act could have a number of adverse effects, including:

- Distress and damage to the patients or others affected
- Reputational harm and public loss of confidence in the Trust
- Enforcement action by the Information Commissioner
- Penalties of up to £500,000 for non-compliance
- Legal action and potential liability for compensation claims
- Failure to meet NHS essential standards of quality and safety.

1.4 This Policy describes, in general terms, how the Trust will meet its obligations under the Act. The Policy will be supported by detailed procedures as necessary, describing how its requirements are to be met in the workplace.

1.5 This Policy is consistent with, and complementary to, the existing policies and procedures listed at Appendix 2.

1.6 The Trust treats any breach of this Policy as a serious disciplinary matter, which may result in dismissal or, in the most serious cases, prosecution for a criminal offence.

1.7 Any breaches of this Policy, actual or near misses, shall be recorded and reported as required by the Trust's Adverse Incident Reporting Policy and Serious Incident Policy. Serious breaches will be reported externally and included in the Trust's Annual Report as required by the Department of Health.

Scope of the policy

1.8 This Policy relates to the handling (***processing***) of all information relating to living people who are named or can be otherwise identified in it.

1.9 The Policy applies to information about any person who comes into contact with the Trust and is the subject of any kind of discussion or record. This will include, for example: patients and carers, service users and clients, visitors and relatives; current, past and potential future employees of the Trust, volunteers and people working under any kind of contract; suppliers of goods and services and employees of partner organisations.

1.10 In line with the Data Protection Act 1998, this Policy governs uses of personal information in any form, whether spoken, written, printed or stored on computer. It therefore applies to medical records, personnel and payroll records, other manual files, microfiche/film, pathology results, x-rays, video recordings etc.

2. Definitions/Terms Used in Policy

Words and phrases in ***bold italics*** are defined more fully in the Glossary at Appendix 1.

3. Policy Statement

3.1 General

a) York Teaching Hospital NHS Foundation Trust is committed to the provision of a secure and confidential service in keeping with legal and best practice standards. It does not see data protection as a barrier to the sharing of information where the sharing is necessary and justified, but welcomes the protective framework provided by the Act.

b) The Trust will put in place systems and procedures to fulfil its obligations under the Act, in particular:

- Notification of its processing activities to the ***Information Commissioner*** (see Section 3.2 below) and
- Compliance with the eight enforceable Data Protection principles (Section 3.3).

3.2 Notification

a) The Trust will, on an annual basis, submit a comprehensive ***notification*** of its processing activities to the Information Commissioner.

b) The Trust will put in place review processes to ensure that the notification is kept up to date.

c) The Trust's notification is published on the Information Commissioner's website at www.ico.gov.uk/ESDWebPages/search.asp. The Trust's registration number is **Z4819561.**

d) The Trust's notification does not cover the processing of information about patients receiving private treatment. Notification of this processing is the responsibility of the clinician, acting in a private capacity, who is the ***Data Controller*** for the purposes of the Act.

3.3 The Principles

Principle 1: Information shall be processed fairly and lawfully

a) To satisfy the principle of fairness, data subjects must be made aware why the Trust needs information about

them, how the information is used and to whom it may be disclosed. This is called the fair processing notice and should be supplied at the time the information is first collected.

b) Patients and service users will be informed by a variety of means, for example by the use of leaflets and posters in patient waiting areas, statements in patient handbooks/on survey forms and verbally by those health care professionals providing care and treatment.

c) A fair processing notice should be supplied to job applicants on receipt of their written application for employment with the Trust. During their induction, staff and volunteers should be supplied with sufficient further information to make processing of their personal details fair.

d) Processing may be seen as "lawful" when it complies with all the provisions of the Act (see point e) below), any other relevant legislation (see Appendix 3) and the duty of confidence established in UK case law. Briefly stated, the latter requires that information given with the expectation that it would be kept in confidence, should not be further used or passed on without the consent of the person who provided the information. There are a number of exceptions to this rule, for example where there is a statutory requirement to disclose, and in matters of personal safety or the overriding public interest. The Trust will maintain confidentiality in accordance with the NHS Confidentiality Code of Practice.

e) In accordance with the Trust's Information Governance Strategy and Work Plan, the Trust will periodically review all processing activities to ensure that they are lawful within the terms of the Act. The relevant conditions are listed in Appendix 4.

f) In consultation with the Information Governance team, Departments and Directorates must establish legitimacy before any new processing is carried out – for example, extending the use of personal information already held, sharing it more widely, or starting to collect personal

data for a new purpose. Consideration will be given to whether the project requires a full-scale or a small-scale Privacy Impact Assessment, in accordance with guidance issued by the Information Commissioner.

Principle 2 – Personal data shall be obtained only for specified and lawful purposes.

a) The Trust will specify, in its notification to the Information Commissioner and in its fair processing notices to data subjects, the purposes for which it intends to process personal data. Purposes will include, for example, provision of health care, administration of health care services, monitoring and audit etc.

b) All staff must be made aware of the legitimate purposes and that using or disclosing information for any other purpose could constitute a breach of the Act.

c) The Trust will take all reasonable steps to ensure that any person to whom personal data are disclosed, does not use them for any purpose over and above that for which they were provided. To this end, the Trust will continue to develop protocols governing the sharing of information with partner organisations.

Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

a) Every item of information collected from individuals must be justified i.e. required for the purpose it is being requested.

b) No item of information should be passed on to any third party unless it is absolutely required. In particular, information which identifies individuals should be removed wherever possible.

c) Staff should be alert to any gaps in the information and make every effort to complete the record by reference to the data subject or other authoritative source.

Principle 4 – Personal data shall be accurate and, where necessary, kept up to date

a) The Trust will take all reasonable steps to ensure that all personal information held on any media is fit for purpose. The Trust's separate Data Quality Policy sets out the measures to be taken in respect of patient information, including the development of data definitions, standards and procedures for data capture, routines for validation and quality assurance, and the regular monitoring and audit of data held in the Core Patient Database.

b) Staff should check with patients that the information held by the Trust is kept up to date by asking patients attending appointments or being admitted to hospital, to validate the information held.

c) Staff information should also be actively maintained and staff have a responsibility to ensure that their manager and/or the Payroll Department are advised of any change to their personal details.

Principle 5 - Personal data shall not be kept for longer than necessary for the stated purpose

a) The Trust will ensure that records of all kinds are actively managed, and that personal information is kept no longer than necessary.

b) The Trust's Records Manager is responsible for developing the Trust's Records Management policy and guidance The Records Manager will also offer advice to Departments and Directorates on all records management matters.

c) Retention periods for all types of manual records are set out in the Trust's Retention Schedule , which forms part of the Records Management Policy and can be found on the Intranet.

d) Disposal of confidential material should be carried out according to the Trust's Destruction of Confidential Waste Policy.

Principle 6 – Personal data shall be processed in accordance with individuals' rights

a) The Trust will make provision for the rights of individuals under the Act. Briefly stated, these are:

- The right of subject access (further information see b) below)
- The right to prevent processing likely to cause harm or distress
- The right to prevent processing for the purposes of direct marketing
- Rights in relation to ***automated decision taking***
- The right to take action for compensation if the individual suffers damage
- The right to take action to rectify, block, erase or destroy inaccurate data
- The right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

b) Individuals about whom information is held within the Trust, have a general right of access to it. This right of access is not automatic, but requires that formal procedures are followed. This ensures that the interests of the data subject, and any other persons identified in the information, are protected. The Trust operates secure Subject Access procedures for both patient and staff information, operated by the Health Records department and Human Resource Directorate respectively. Both can be found on the Intranet.

c) The Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased patients' records.

d) Individuals also have a right to complain if they believe that the Trust is not complying with the requirements of

the Data Protection legislation. Any such complaints will be dealt with through the formal complaints procedure, and resolved in consultation with the Information Governance team.

Principle 7 – personal data shall be kept securely

a) All information relating to identifiable individuals must be kept secure at all times. The Trust will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information.

b) Appropriate countermeasures will include, for example:

- system and network security,
- physical and logical access controls,
- ***safe haven*** procedures,
- formal contracts with other organisations who process personal data on behalf of the Trust,
- clauses in employment and honorary contracts and
- staff training.

c) Detailed requirements are set out in the Information Security Policy, supported by further policies and Staff Guides as listed in Appendix 2. A summary is made available to all new starters in the Information Security Handbook and all security policies and guidance are published on the Intranet.

Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area without an adequate level of protection

a) The Trust will seek, wherever possible, to avoid sending personal information outside of the EEA. Patients seeking treatment abroad will normally be asked to

submit a subject access request to obtain copies of their notes.

b) To ensure that proper safeguards are in place, any proposal to send personal data to countries outside of the EEA must be discussed with the Information Governance Manager.

4. Equality Impact Assessment

4.1 The Trust's statement on Equality is available in the Policy for Development and Management of Policies at Section 3.3.4.

4.2 A copy of the Equality Impact Assessment for this policy is at Appendix 5.

5. Accountability

5.1 Overall accountability for Data Protection in York Teaching Hospital NHS Foundation Trust lies with the Chief Executive. He must account for the data processing activities of the organisation, which is a Data Controller under the terms of the Act.

5.2 The Director of Nursing is the Trust's designated lead director for Information Governance issues, including Data Protection.

5.3 As Senior Information Risk Owner for the Trust, the Director of Finance takes ownership of the organisation's ***information risk management*** policy and strategy.

5.4 The Trust's Medical Director fulfils the role of Caldicott Guardian, having lead responsibility at Board level for the protection, use and sharing of patient-identifiable information.

5.5 In accordance with Data Set Change Notice 18/2009, the Trust has a named IT Clinical Risk Lead, who is charged with ensuring the clinical safety of any new IT system. In particular, the role ensures the quality of patient data used to support clinical decision-making.

5.6 The Assistant Director of Healthcare Governance has delegated responsibility for the Trust's confidentiality and data protection work programme, and chairs the Information Governance Group. Supported by a team of Information Governance specialists, the Assistant Director of Healthcare Governance ensures that the following functions are carried out to nationally-agreed standards:

- Maintenance of the Trust's notification to the Information Commissioner
- Reviews of processing to ensure compliance with the Principles
- Development of Data Protection policies and procedures
- Design and delivery of core Data Protection training, including induction
- Oversight of the Data Protection component of Research Governance
- Provision of data protection advice and guidance
- Reporting of progress both internally and externally to NHS Connecting for Health and the Care Quality Commission.
- Information Governance issues, including Data Protection, are overseen by the Trust's Information Governance Group, which reports to the Board of Directors via the Corporate Risk Management Group.

5.7 Working together with the Information Governance team, Departments and Directorates are responsible for the implementation of this Policy. In particular, they should ensure that:

- Data Protection and confidentiality credentials are considered during the recruitment of new staff.
- Staff receive adequate training in Data Protection. Mandatory training requirements are as specified in the Trust's Statutory and Mandatory Training Identification

Policy. New starters will attend an Information Governance (IG) signposting session, supplemented by:

a) completion of the Introductory module of the IG E-learning tool, accessible on the Trust's Learning platform, and

b) further job-specific guidance as set out in the Induction Checklist (part of the Recruitment, Appointment and Selection Policy). There is a separate Junior Doctors' Corporate Induction Policy.

The ongoing training needs of established staff will be met through the annual Information Governance Training and Awareness Plan. Formal Training Needs Analysis will be used to identify and address any additional support required by specific staff groups.

- Personal data are collected and used according to documented Safe Haven standards and procedures. Procedures governing the recording of data onto CPD have been agreed at corporate level and are available on Horizon.

- Patients and staff are supplied with the Fair Processing information.

- Staff are prepared to deal with, or direct appropriately, any queries relating to the use of personal information, or Subject Access requests.

- Proper support is provided to Information Governance staff conducting IG compliance reviews, surveys and mapping exercises, and priority given to implementing any resulting action plans.

- Computer security rules are observed and any breaches of security reported via DatixWEB.

- Any planned changes in the processing of personal data are consistent with this Policy and are carried out in consultation with the Information Governance team.

5.8 Every employee of the Trust has a fundamental responsibility to protect the personal information they work with, or come into contact with in the course of their duties.

This is a common, legal and contractual duty, which is clearly stated in the Trust's Information Governance policies.

6. Consultation, Assurance and Approval Process

6.1 The consultation, assurance and approval process is detailed in section 6 of the Policy for the Development and Management of Policies.

6.2 This Policy has been prepared by reference to the Data Protection Act 1998, other legislation and NHS guidance as listed in Appendix 3.

6.3 Consultation was made with the then Information and Records Management Committee prior to publication of the original Policy. On the Committee, now the Information Governance Group, are the Trust's Medical Director and Caldicott Guardian, senior consultants from a range of disciplines, the Senior Information Risk Owner, the Director of Systems & Network Services, the Head of Risk and Legal Services, Head of Patient Access and representation from a range of departments and directorates.

6.4 Additionally, consultation has been made with the following:

- Human Resource Directorate and staff organisation representatives,
- Internal Audit
- Patient Experience
- Corporate Learning and Development.

7. Review and Revision Arrangements

7.1 The date of review is given on the front coversheet.

7.2 Persons or group responsible for review are:

- Policy author and owner
- Information Governance Group

7.3 The Healthcare Governance Directorate will notify the author of the policy of the need for its review six months before the date of expiry.

7.4 On reviewing this policy, all stakeholders identified in section 6 will be consulted as per the Trust's Stakeholder policy. Subsequent changes to this policy will be detailed on the version control sheet at the front of the policy and a new version number will be applied.

7.5 Subsequent reviews of this policy will continue to require the approval of the appropriate committee as determined by the Policy for Development and Management of Policies.

8. Dissemination and Implementation

8.1 Once approved, this policy will be brought to the attention of relevant staff as per the Policy for Development and Management of Policies, section 8 and Appendix 6 Plan for Dissemination .

8.2 This policy is available in alternative formats, such as Braille or large font, on request to the author of the policy.

8.3 This Policy will be team briefed across the organisation and will be published on the Intranet, along with detailed guidance as to how compliance can be achieved. Other channels will be used to communicate the Policy to all staff, including the IG Newsletter BIG News, awareness events, e-mail and periodic articles in Team Brief and Staff Matters.

8.4 Policy requirements will be incorporated into induction, Statutory and Mandatory training and IT training, all of which are compulsory for all Trust staff. Subject specialists will design and deliver additional training as required by published Information Governance requirements.

9. Document Control including Archiving

The register and archiving arrangements for policies will be managed by the Healthcare Governance Directorate. To

retrieve a former version of this policy the Healthcare Governance Directorate should be contacted.

10. Monitoring Compliance and Effectiveness

Compliance with the Policy is managed as follows:

Evidence	Monitoring /Who by	Frequency
a. In-year, progress against the Information Governance Improvement Plan	Information Governance Group Corporate Risk Management Group	Quarterly
b. Audit Report – IG Toolkit evidence	Internal Audit External Audit	Annually On direction of CfH
c. Assessment results (Toolkit submission)	NHS Connecting for Health Care Quality Commission Audit Commission Monitor	Three times annually (July, October, March) Annually
d. Compliance reviews	Assistant Director of Healthcare Governance	Rolling programme
e. Incident Reports	Information Governance Group	Quarterly
f. SIRO Report	Board of Directors	Annually

10.2 Standards / Key Performance Indicators

- Data Protection Act 1998

- Information Governance Toolkit (NHS Information Centre)

11.Training

In accordance with Information Governance Toolkit requirements, appropriate IG training is delivered to all staff on an annual basis. The IG training needs of particular staff groups will be identified through an annual IG Training Needs Analysis, linked to the corporate TNA.

Corporate and local induction procedures, along with mandatory IT training, will introduce new starters to the main provisions of this policy. Existing staff will receive annual IG refresher training delivered as part of the Statutory and Mandatory programme.

12.Trust Associated Documentation

The full text of the following locally-developed guidance can be found under 'Policies and procedures' on the Trust Intranet, or obtained by contacting the Information Governance Team on (01904 72) 5306.

- Information Governance Policy
- Data Quality Policy
- Information Security Policy
- Management and Maintenance of Records Policy and Guidance
- Information Governance Staff Guides Series:
    1. Information Governance and You
    2. Confidentiality Code of Conduct
    3. Safe Haven Guide
    4. Laptop Security
    5. Emailing Personal Information
    6. Mobile Working
    7. Clinical Record Keeping Standards:
        a. Scarborough Hospital
        b. York Hospital
    8. Records Management
    9. Data Protection

10. Accessing Information About You
11. Freedom of Information
12. Information Security Incidents
13. Sharing Information with the Police
14. Use of Social Networking Sites

Standard Operating Procedure (SOP) for Information Governance Review of Research Governance Applications

BIG News – Information Governance Newsletter

N.B. This list is not exhaustive as new policies are being developed at time of writing. Please look on the Intranet for updates.

Departments and Directorates will have further local procedures in support of these Policies.

13. External References

The Data Protection Act 1998 - http://www.legislation.gov.uk/ukpga/1998/29/contents

Information Commissioner's Office – http://www.ico.gov.uk/Default.aspx

NHS Confidentiality Code of Practice, Department of Health, 2003 http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4069254.pdf

14. Appendices

As set out in Contents List

Appendix 1 – Glossary of Terms

Automated decision taking
A method of decision making taking place without human judgement
(such as computer produced shortlists for interviews resulting from automated psychometric testing, or credit rating spot checks run against postcodes)

Consent
Agreement by an individual to proceed with processing, freely given, with an understanding of the risks, benefits, limitations, and potential implications of the processing

Data Controller
A person who determines the purpose for which and the manner in which any personal data are, or are to be processed. A "person" may not mean a living individual – it refers to a legal person i.e. an organisation – in our case, York Teaching Hospital NHS Trust.

Data Subject
A living individual who is the subject of personal data

Explicit consent
Full, clear and express consent given by the subject to process data for a specific and defined purpose other than those for which consent has already been agreed. Explicit consent can sometimes legitimise the processing and may be called upon as a record of such. Best Practice is to obtain a signature.

Information Commissioner
The Information Commissioner enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000. The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. In the UK the Commissioner has a range of duties including the promotion of good information handling and the encouragement of codes of practice for data controllers, that is, anyone who decides how and why personal data, (information about identifiable, living individuals) are processed.

Information Risk Management
Information risk management is concerned with protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. Information risk is managed through identified Information Asset Owners, who are responsible for carrying out regular assessments, and providing assurances to the Senior Information Risk Owner.

Notification
Notification is the process by which a data controller informs the Commissioner about the nature of his processing of personal data. The data controller must say what information he holds about what categories of individual, for what purposes, and who the information may be disclosed to. Details are published in a register which is available to the public for inspection. Notification, therefore, serves the interests of data controllers in providing a mechanism for them to publicise details of their processing activities, and also serves the interests of data subjects in assisting them to understand how personal data are being processed.

Personal Information
Personal information means information which relates to a living individual who can be
identified from that information, or from that information and other information which
is in the possession of, or is likely to come into the possession of, the data controller.

Processing
Processing means obtaining, recording or holding the data or carrying out any
operation or set of operations on the data. It includes organising, adapting and
amending the data, retrieval, consultation and use of the data, disclosing and
erasure or destruction of the data. It is difficult to envisage any activity involving data which does not amount to processing.

Safe Haven
A location (or system) within an organisation where arrangements and procedures are in place to ensure personal information can be

held, received and communicated securely. The Trust's Safe Haven procedures set out the required standards for use of e-mail, fax and post, as well as for physical security of patient and staff records.

Sensitive personal data
Defined in the Act as personal data relating to: Racial or ethnic origin, political opinions, religious beliefs (or similar), trade union membership, physical or mental health, sexual life, commission, or alleged commission of offences, proceedings for any offence or alleged offence.

Appendix 2 – Related Legislation and Guidance

1. The Human Rights Act 1998

Article 8 of the European Convention on Human Rights, incorporated into UK Law by the Human Rights Act 1998, gives people the right to respect for their private and family life, their home and their correspondence. The HRA enabled UK courts to hear actions, brought by individuals, in relation to human rights issues.

2. The Access to Health Records Act 1990

This Act was largely superseded by the 1998 Data Protection Act but continues to provide for access to the records of deceased persons.

3. Section 251 of the NHS Act 2006

Section 251 of the NHS Act 2006 re-enacted Section 60 of the Health and Social Care Act 2001. The terms Section 60 and Section 251, when used in relation to use of patient information therefore refer to the same powers. These powers allow the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for medical purposes, such as research, where it is not possible to use anonymised information and where seeking individual consent is not practicable. Under the Health and Social Care Act 2008, responsibility for administering these powers was transferred from the Patient Information Advisory Group to the National Information Governance Board.

4. The Freedom of Information Act 2000

This Act gives everyone a legal right to see information held by public bodies, including national, regional and local government and the NHS. Its aim is to open up public organisations to public scrutiny and to make them more accountable. The Information Commissioner is responsible for implementing the Act in England and Wales and more information is available on the IC website. NHS organisations came within the scope of the FOI in October 2003. Trusts must have in place publication schemes to demonstrate openness in their day-to-day business, and procedures for dealing with individuals' requests for additional information. Under the FOI Act, individuals have the right to ask for any information held by public bodies, and to have it supplied unless it is exempt for any reason (such as national security).

5. The Computer Misuse Act 1990

This is the UK's anti-hacking, anti-snooping, anti-virus legislation. It gives organisations the right to prosecute people who access their computers without proper authorisation or who try to corrupt their software or data. The Trust reserves the right to take disciplinary and possibly legal action against any member of staff who exceeds their authority to access and amend information held on computer.

6. The Copyright, Designs and Patents Act 1988

This law was passed to protect intellectual property. It means that unauthorised copying of computer software is a criminal offence. Policy requires that all software used on computers belonging to the Trust is properly authorised and licensed for the intended use. Software installations will be subject to periodic audit and copies of licence documentation must be available for review.

7. The Mental Capacity Act 2005

The Mental Capacity Act 2005 came fully into force in 2007 and provides a framework to empower and protect people who may lack capacity to make decisions themselves, for example individuals with dementia, learning difficulties, mental health problems, stroke or head injuries. The Act enables people to make advance decisions regarding their treatment in the event that they later lose capacity to consent. In addition, the Act deals with the situation in which designated decision-makers can act on behalf of an individual who cannot consent themselves. It does this by creating LPAs (Lasting Powers of Attorney), superseding Enduring Powers of Attorney.

OTHER LEGISLATION

Processing may also be subject to additional UK laws including:

o The Crime and Disorder Act 1998

o The Regulation of Investigatory Powers Act 2000

o The Electronic Communications Act 2000

o The Privacy and Electronic Communications Regulations 2003, amended 2011.

o NHS Trusts (Venereal Diseases) Directions 1991

o NHS (Venereal Diseases) Regulations 1974

More information can be found on the Intranet and via links to the Internet.

Websites

The Information Governance Toolkit at https://nww.igt.connectingforhealth.nhs.uk/

The Information Commissioner's Website at http://www.ico.gov.uk/

Appendix 3 – Conditions for Lawful Processing

Under the terms of the Data Protection Act, for any processing of personal data to be lawful, at least one condition from Schedule 2 of the Act must be met. These are, in brief:

- Consent of the data subject
- Contractual necessity
- Non-contractual legal obligation of the ***data controller***
- To protect the vital interests of the data subject (i.e. in a case of life or death)
- Functions of a public nature e.g. as conferred by enactment ***or***
- In the legitimate interests of the data controller.

In the case of ***sensitive personal data*** – that is, information relating to a person's mental or physical health, sexual life, racial or ethnic origin, religious beliefs, trade union membership or any criminal convictions or proceedings – tighter conditions apply. In particular, one of the conditions listed in Schedule 3 of the Act must be met *in addition to* one of the Schedule 2 conditions listed above. The Schedule 3 conditions include the following, most likely to be relevant to the Trust:

- The data subject has given their *explicit* consent – wherever possible evidenced by signature
- Legal duty imposed on employers e.g. monitoring of ethnicity
- Life and death issues
- Information already put in public domain by data subject
- Processing necessary in relation to legal rights or for the administration of justice

- Processing necessary for the exercise of any function conferred by enactment

- Processing necessary for medical purposes including diagnosis, care and treatment and management of healthcare services (but the processing still has to be fair and in keeping with the duty of confidence – i.e. a measure of choice should normally be provided.)

Appendix 4: Equality Impact Assessment Tool

To be completed when submitted to the appropriate committee for consideration and approval.

Name of Policy:	Information Governance Policy

1.	**What are the intended outcomes of this work?** To inform staff how to effectively manage information in a secure and accurate manner.	
2	**Who will be affected?** All staff and patients, enquirers.	
3	**What evidence have you considered?** *List any examples of good practice you have used in putting this policy together, ensuring consideration to the ability to implement the policy by the following groups has been given* Principal model is national policy as represented in Connecting for Health's Information Governance Toolkit. The Policy is designed to protect the information rights of all people, including protected groups.	
a	**Disability** In this and related policies, provision has been made for those who may lack capacity to consent in relation to information sharing and use.	
b	**Sex** This policy is inclusive and does not differentiate between people on the basis of this characteristic.	
c	**Race** This policy is inclusive and does not differentiate between people on the basis of this characteristic.	
d	**Age** . This policy is inclusive and does not differentiate between people on the basis of this characteristic.	
e	**Gender Reassignment** This policy is inclusive and does not differentiate between people on the basis of this characteristic.	
f	**Sexual Orientation** This policy is inclusive and does not differentiate between people on the basis of this characteristic.	
g	**Religion or Belief** This policy is inclusive and does not differentiate between people on the basis of this characteristic.	
h	**Pregnancy and Maternity**. This policy is inclusive and does not differentiate between people on the basis of this characteristic.	
i	**Carers** This policy is inclusive and does not differentiate between people on the basis of this characteristic.	

j	**Other Identified Groups** None	
4.	**Engagement and Involvement**	
a.	Was this work subject to consultation?	Yes
b.	How have you engaged stakeholders in constructing the policy	Via consultation with Information Governance Group
c.	If so, how have you engaged stakeholders in constructing the policy	As above
d.	For each engagement activity, please state who was involved, how they were engaged and key outputs Medical Director / Caldicott Guardian, Senior Information Risk Owner and representatives of Departments and Directorates on the Information Governance Group Outputs = review, approval, systems for training and compliance monitoring	
5.	**Consultation Outcome** *Now consider and detail below how the proposals impact on elimination of discrimination, harassment and victimisation, advance the equality of opportunity and promote good relations between groups*	
a	Eliminate discrimination, harassment and victimisation	Makes information rights available to all
b	Advance Equality of Opportunity	Makes information rights available to all
c	Promote Good Relations Between Groups	Encourages dialogue between Trust and service users
d	What is the overall impact?	Information rights available to all
	Name of the Person who carried out this assessment: Susan Hall, Information Governance Manager	
	Date Assessment Completed 2nd December 2012	
	Name of responsible Director Libby McManus	

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Equality and Diversity Committee, together with any suggestions as to the action required to avoid/reduce this impact.

Appendix 5 Checklist for Review and Approval

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1	**Development and Management of Policies**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or procedures?	Yes	
2	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3	**Development Process**		
	Is the method described in brief?	Yes	
	Are individuals involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Has an operational, manpower and financial resource assessment been undertaken?	Yes	
4	**Content**		
	Is the document linked to a strategy?	Yes	
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and	Yes	

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	unambiguous?		
5	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are local/organisational supporting documents referenced?	Yes	
5a	**Quality Assurance**		
	Has the standard the policy been written to address the issues identified?		
	Has QA been completed and approved?	Yes	
6	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate, have the staff side committee (or equivalent) approved the document?	N/a	
7	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8	**Document Control**		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9	**Process for Monitoring Compliance**		

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	Are there measurable standards or KPIs to support monitoring compliance of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so, is it acceptable?	Yes	
11	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	Yes	

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Fiona Jamieson	Date	17th January 2013
Signature			
Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Fiona Jamieson	Date	17th January 2013
Signature			

Appendix 6 Plan for dissemination of policy

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Title of document:	**Information Governance Policy**
Date finalised:	**January 2013**
Previous document in use?	**Yes**
Dissemination lead	**Susan Hall**
Which Strategy does it relate to?	**Information Governance Strategy**
If yes, in what format and where?	**Document held by Healthcare Governance Directorate**
Proposed action to retrieve out of date copies of the document:	**Healthcare Governance Directorate will hold archive**

Dissemination Grid

To be disseminated to:	**1) All Staff**	**2)**
Method of dissemination	**Staff Briefing**	
who will do it?	**IG Team**	
and when?	**Next available**	
Format (i.e. paper or electronic)	**Electronic**	

Dissemination Record

Date put on register / library	**On approval**
Review date	**January 2015**
Disseminated to	**All via Staff Room**
Format (i.e. paper or electronic)	**Electronic**
Date Disseminated	
No. of Copies Sent	**N/A**
Contact Details / Comments	**No substantial change to communicate. Supporting IG Policies set out detailed requirements.**