Information Use Framework Policy

V4.0

November 2016

Summary.

This should be a flow chart that describes the process and shows the accountable person or group at each stage.

For guidance on how to produce a flow chart refer to Appendix 1 of:

Guidance on Producing Mobile Summary Guidance for the RCHT Mobile Guidelines Website - *available via the RCHT Intranet.*

An example of a policy flow chart can be found in the:

Policy for the Development and Management of Knowledge, Procedural and Web Documents (The Policy on Policies)

Table of Contents

1. Introduction

1.1. The Royal Cornwall Hospitals NHS Trust has a legal obligation to comply with all appropriate legislation and guidance issued by the Government in the form of the Office of the Information Commissioner and the Department of Health in connection with data information and IT Security.

1.2. This policy outlines how the Trust will meet its legal obligations in respect of the Data Protection Act 1998, with regard to the residual powers of the Access to Health Records Act 1990, Freedom of Information act 2000 and other appropriate legislation.

1.3. The policy relates to computer systems and manual records including sensitive data involved with medical records, human resources information required to manage staff employment and corporate information held regarding the affairs and running of the Trust.

1.4. Legislation

The main controlling authority is the Data Protection Act 1998 however, the Access to Health Records Act 1990, the Access to Medical Reports Act 1998, Human Rights Act 1998, Freedom of Information Act 2000, Regulation of Investigatory Powers Act 2000, Police and Criminal Evidence Act 1984, Criminal Justice and Immigration Act 2008 and the Crime and Disorder Act 1998 also impact on the Trust's responsibilities to manage personal data.

1.5. NHS Guidance

The following circulars also apply:

1.6. IMG:E5498 Ensuring Security and Confidentiality in NHS Organisations HSG(96)18 The Protection and Use of Patient Information HSG 1999/012 Caldicott Guardians HSC 2002/003, Caldicott review 1 & 2: information governance in the health and care system, Implementing the Caldicott Standard into Social Care, HSC 1999/053 NHS Code of Practice mentioned in 1.8, HSC 1998/217 Preservation, Retention and Destruction of GP General Medical

1.7. DoH NHS Code of Conduct in Respect of Confidentiality Nov 2003: Records Management: NHS Code of Practice March 2016

1.8. Data Protection Act 1998

The Trust has a duty under the Data Protection Act to hold, obtain, record, use and store all personally identifiable information in a secure and confidential manner. This applies to all personally identifiable information held in manual files, computer databases, videos and other automated media about living individuals such as Human Resources and payroll records, medical records, other manual files, microfilm/fiche, pathology results, images and other sensitive data.

1.9. The Act states that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside of their employment responsibilities. Any unauthorised disclosure of information by a member of staff will be considered to be a disciplinary offence.

1.10. The DPA also requires the Trust to register the data that it holds with the Office of the Information Commissioner. This registration identifies the purpose for holding the data, how it is used and to whom it may be disclosed. The Act embodies eight Data Protection Principles formally guiding the management of data.

1.11. Freedom of Information Act 2000

1.12. The Freedom of Information Act 2000 (FOIA) gives a general right of access to recorded information held by public authorities, sets out exemptions from that right, and places a number of obligations on public authorities, such as the Royal Cornwall Hospitals NHS Trust, to:

1.13. Have a Publication Scheme setting out what information will be made routinely available to the public; and

1.14. Respond positively to requests from the public for information, unless that information is explicitly exempt.

1.15. All types of information are covered by the FOIA including documents that are not held in 'structured systems' (unlike the Data Protection Act). It is generally a fair assumption that all information will need to be made available unless a valid reason exists for it to be withheld.

1.16. Environmental Information regulations (EIR)

The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities.
The Regulations do this in two ways:

- public authorities must make environmental information available proactively;
- members of the public are entitled to request environmental information from public authorities.

1.17. The Regulations give people a right of access to information about the activities of public authorities that relate to or affect the environment, unless there is good reason for them not to have the information.

1.18. This version supersedes any previous versions of this document.

2. Purpose of this Policy/Procedure

2.1. This policy sets out the legislative and operational framework which governs the application of Data Protection ,FOIA and EIR, together with the internal processes through which the RCHT will manage its compliance. It is intended to:

2.2. Facilitate disclosure of information under the DPA 1998, FOIA 2000 and EIR by setting out the procedures the RCHT will follow

2.3. To ensure the safe transmission and receipt of information through designated Safe Havens.

2.4. Serve the interests of data subjects and applicants for information, by setting out standards for the provision of advice, and to ensure there is an effective means of complaining about decisions taken.

2.5. Provide RCHT staff with clear guidance on handling and dealing with requests for information so that the RCHT is able to meet its obligations under these Acts.

3. Scope

3.1. This policy is applicable to all staff of the Trust as every member of staff has a responsibility for handling either personal identifiable data or corporate records. It is also intended that those working as contractors of providers of services should also adhere to the provisions of this policy.

3.2. This framework document covers all data and information whether held electronically or on paper.

4. Definitions / Glossary

DPA. Data Protection Act 1998.
GDPR. General Data Protection Regulations (coming in to force May 2018)
FOIA. Freedom of Information Act 2000
Information. Any record held in any form regardless of its source, production date or location this includes, but is not limited to, all paper and electronic documents, video and audio recordings.
Explicit or Absolute Exemption. Certain information cannot be disclosed and is therefore subject to an absolute exemption.
Qualified Exemption. The disclosure of certain information can be refused following the application of a public interest test. This is known as a qualified exemption.
Vexatious Request. There are various factors that could lead to a request being considered vexatious and, if in any doubt, specialist advice should be sought. Public bodies do not have to respond to vexatious requests and there is no public interest test.
Repeated Request. To be considered a Repeated Request the request must be made by the same person, be substantially similar to previous requests and should have been submitted without a reasonable period having elapsed since the previous request
Round-Robin Request. Round-robin requests are enquiries, sometimes in the form of a questionnaire, which were being circulated to numerous authorities in the same sector
PID, Patient Identifiable Data, that which can be used to uniquely identify an individual either directly or through use with other information which maybe in the data processors procession.
IG. Information Governance. The framework which brings together best practice, legislation and guidance in order to protect and promote confidentiality.
IGC. Information Governance Committee which monitors progress against IG Toolkit compliance.
IGT. Information Governance Toolkit used to provide assurance through the collection of evidence based compliance against a range of standards.
Primary Uses – is when information is used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.
Secondary Uses – is for non-healthcare and medical purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When PID is used for secondary use this should be limited and de-identified so that the secondary uses process is confidential.
Pseudonymisation – The technical process of replacing person identifiers in a dataset with other values (pseudonyms) from which the identities of individuals

cannot be intrinsically inferred e.g. the replacement of an NHS number with another random number. Pseudonymisation may be reversible or irreversible

Safe Haven –

- An environment which is secure and is controlled. This ensures that the use of person information is subject to the same strict controls, which already apply elsewhere, where confidential information is handled. There is a requirement to reassure patients, staff and the public that information will be handled securely and safeguards are in place to ensure its security
- A process of ensuring information is secured through appropriate safeguards (e.g. role based access, anonymised or pseudonymised data) to restrict access to data sets containing personal or confidential information.

Privacy Impact Assessment – A tool to ensure all aspects of privacy are considered as part of any new project or one that involved significant changes where personal data is likely to be processed.

5. Ownership and Responsibilities

5.1. *Chief Executive*

The Chief Executive is responsible for:

- Ensuring appropriate and qualified resources are in place to manage DPA requirements;
- Agreeing any undertakings or enforcement notices which could be sanctioned by the Information Commissioner;
- Ensuring an effective policies for Data Protection and Freedom of Information Act is in place within the Trust;
- Deciding whether an S36 (FOIA) exemption may legitimately be applied to a specific request for information received by the Trust.

5.2. *Head of Corporate Compliance*

The Head of Corporate Compliance (IG Lead) acts as the Trusts Data Protection Officer and Freedom of Information Lead. This role is responsible for:

- Promoting adherence with regard to all aspects of the IG Toolkit, which includes compliance with the DPA, FOIA/EIR and Pseudonymisation guidance.
- Ensuring staff are aware of their obligations under the DPA and FOI through mandatory training and supporting communications and training material.
- Monitoring compliance with regard to this policy (and associated policies).
- Chairing the Information Governance Committee.
- Working with the Caldicott Guardian and Senior Information Risk Officer to ensure compliance with relevant legislation.
- Working closely with the Records Services, PAS & Data Quality Manager, Corporate Records Manager, IT Security Manager and the Information Asset Owners to ensure information is being managed appropriately.
- Provides the Trust with expert IG advice, administrative leadership of the programme and the first point of contact for staff on IG matters.
- Promoting and ensuring Safe Haven areas are maintained and ensuring best practice is known by those operating in these areas.

5.3. *Information Services Manager*

The Information Services Manager is responsible for

- The new safe haven concept and ensuring that only staff with a genuine business need have access to patient level information accessible through tools provided or created by the Information Services Team.
- Developing the Trusts preferred delivery tool to ensure access controls are implemented.

5.4. *Role of the Medical Director/Caldicott Guardian*

The Trusts Medical Director is the Caldicott Guardian and has a dual role to play.

The post holder has a particular responsibility for:

- Reflecting the patients' and staff interests regarding the use of personal information. He/she is responsible for ensuring personal identifiable information is stored and shared in an appropriate and secure manner.
- The Medical Director has operational responsibility for clinical record keeping standards for the consultant/doctor body of staff.
- Deciding in partnership with the SIRO as to whether data breaches have the desired construct to be reported to the Information Commissioners Office.

5.5. *Role of the Director of Health Informatics and ICT*

The Director of ICT is responsible for:

- Ensuring the requirements of the IG Toolkit are embedded in Project Management practices (e.g. Privacy Impact Assessments)
- Ensuring technical services are implementing IG approved processes for software installation and management.
- Ensuring appropriate resources are in place to meet the demands of ensuring compliance with the technical elements of the IG Toolkit to a minimum of Level 2.

5.6. *Role of the Corporate Records Manager*

The Trust's Corporate Records Manager holds:

- Day-to-day responsibility and reports to the Records Services, PAS & Data Quality Manager for delivery of corporate records management.
- The Corporate Records Manager will advise on policy and best practice and is responsible for ensuring the creation and implementation of records management tools and guidelines and that records management systems and processes are developed, co-ordinated and monitored.
- Ensuring the requirements of the IG Toolkit are met.

5.7. *Role of the Managers*

Line managers are responsible for:

- Ensuring all staff within their division are aware of this policy and have read it;
- Ensuring all staff within their division are complaint with this policy;
- Reporting any risks or incidents which this policy has a bearing on;
- Ensuring that all staff adhere to the precepts of Pseudonymisation as well as to the Caldicott principles and the Data Protection Act 1998;
- Ensuring that access to patient level information is agreed only where it is required to enable staff to perform their role (via sign off on relevant access forms).

5.8. *Role of the Information Governance Committee*

The Information Governance Committee is responsible for:

- Overseeing the Information Governance agenda and represents the interest of the RCHT. It includes working with Responsible Authorities and other vested stakeholders in determining and ratifying Information Sharing Protocols ensuring the best interest of the RCHT, patients, the public and of the functions of business are served. It monitors progress towards the annual sign-off of RCHT IGT self-assessment obligations and receives and acts on breaches of confidentiality and information security. The committee is responsible for approving and ratifying policies, as well as identifying risks in relation to its core business and ensuring that they are being managed appropriately. Data Protection and Freedom of Information forms part of this regular agenda.
- The IGC ensures the Trust is compliant with all aspects of legislation with regard to DPA and FOIA.

5.9. *Role of Individual Staff*

All staff members are responsible for:

- Creating and maintaining records, which are accurate, appropriate and retrievable;
- Adhering to the legislation covering their daily activity. (e.g. DPA, FOIA)
- Reading local policies and procedures relevant to their posts.
- Ensuring that requests made under FOI or DP are passed in a timely manner to staff that are responsible for responding to such requests;
- Ensuring that disclosures are not made outside of the defined process, so that inappropriate disclosures are avoided;
- Reporting breaches of confidentiality to the Data Protection Officer.
- Reporting Risks and Incidents which could lead to failure to comply with the policy of legislation on the Trusts Incident and Risk reporting tool, Datix.
- Ensuring that documents that are within the classes of information of the Trust's FOI publication scheme are provided for publication;
- Bringing new corporate documents or classes of information that have not been previously published to the attention of the Freedom of Information Lead who will facilitate agreement on publication of such material(s);
- Staff responsibilities will be set out in contracts of employment. A breach of these responsibilities could result in disciplinary action.
- All staff coming into contact with person identifiable information must ensure the movement of information is carried out in a secure manner in line with all trust policies and procedures.

- Ensuring that they abide by the precepts of Pseudonymisation and Safe Haven conditions.
- To not access or use any information that they do not have a legitimate relationship with.
- To not use any information gathered by the Trust in any activity that does not meet the Trusts objectives. No Trust data is to be used for personal use or for financial gain without the express permission of the Head of Corporate Compliance and/or appropriate Board Director.

5.10. *Senior Information Risk Officer*

- Provides the board-level lead on Information Governance and is responsible for overseeing any Trust IG or data handling risks.
- Agreeing in partnership with the Caldicott Guardian whether incidents have the right construct to be reported to the Information Commissioners Office.

5.11. *IT Security Manager*

- Is responsible for providing expert advice and support in delivering the technical assurance for IGT compliance.

5.12. *PAS, Data Quality & Records Services Manager,*

- Is responsible for delivering appropriate records management (Health) within the Trust to conform to the IG standards.
- Is responsible for delivering appropriate data quality management within the Trust to conform to the IG standards

6. Standards and Practice

There are a number of standards of practice that this policy covers; these can be found in the appendix as shown.

- Data Protection Policy – Appendix 1
- Freedom of Information Policy. – Appendix 2
- Pseudonymisation Policy. – Appendix 3
- Information Governance Policy – Appendix 4
- Safe Haven Policy – Appendix 5

7. Dissemination and Implementation

7.1. This policy will be published on the Trust Document Library following authorisation by the Executive Director. Immediately following publication the Head of Corporate Compliance will ensure that its publication is highlighted across the Trust using various media including the records management newsletter and all users bulletin. Implementation of this policy will be supported through a series of briefings, departmental visits and training as required.

7.2. Trust staff will be made aware of their responsibilities for data protection and Freedom of Information through generic and specific training programmes and guidance. These will include the Corporate Induction and mandatory training programmes.

7.3. All new staff members, and those returning to work after a period of absence, are required to attend the Trust corporate induction programme which includes a

session on Information Security and Records Management. Attendance at this session will enable staff to understand their responsibilities with respect to records management, handling information, information security, and confidentiality.

8. Monitoring compliance and effectiveness

Element to be monitored	The effectiveness of the Standards of Practice for each section will be monitored and reported on as required.
Lead	Head of Information Governance supported by various committees.
Tool	Compliance with the requirements of the IG Toolkit and legislation covering Data Protection and Information Governance. The delivery tool will be papers tabled at the Trusts Information Governance Committee.
Frequency	Monitoring will be on-going. Reports will be delivered bi-monthly to the IGC. Adverse reports will be shared as and when they are created.
Reporting arrangements	Information Governance Committee Each area of this framework document is covered by specific agenda items at the IGC. The Head of Information Governance is expected to read and interrogate the report to identify deficiencies in the system and act upon them
Acting on recommendations and Lead(s)	TMCG will receive reports highlighting key area of achievement or concern. Required actions will be identified and completed in a specified timeframe
Change in practice and lessons to be shared	Depending on the area for improvement or action, lessons learnt will be given appropriate consideration and discussion through committee or made available through public awareness mechanisms. A lead member of the team will be identified to take each change forward where appropriate. Lessons will be shared with all the relevant stakeholders

9. Updating and Review

9.1. This Policy will be revised every 3 years by the Head of Corporate Compliance in conjunction with the Records Services, PAS & Data Quality Manager, Head of Information Services and the Corporate Records Manager.

10. Equality and Diversity

10.1.This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the 'Equality, Diversity & Human Rights Policy' or the Equality and Diversity website.

10.2.Royal Cornwall Hospitals NHS Trust is committed to a Policy of Equal Opportunities in employment. The aim of this policy is to ensure that no job applicant or employee receives less favourable treatment because of their race, colour, nationality, ethnic or national origin, or on the grounds of their age, gender, gender reassignment, marital status, domestic circumstances, disability, HIV status, sexual orientation, religion, belief, political affiliation or trade union membership, social or employment status or is disadvantaged by conditions or requirements which are not justified by the job to be done. This policy concerns all aspects of employment for existing staff and potential employees.

10.3. *Equality Impact Assessment*

10.4. The Initial Equality Impact Assessment Screening Form is at Appendix 6.

Appendix 1. Data Protection Policy Standards and Practice

1. Security & Confidentiality

All information relating to identifiable individuals and any information that may be deemed sensitive, must be kept secure at all times. Royal Cornwall Hospitals Trust will ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information

Database Management

The Royal Cornwall Hospitals Trust Data Protection Officer will ensure that all databases that require registration are registered in accordance with the Act's requirements and these registrations are reviewed on a regular basis. Each computer system/database will have a designated manager. A list of these nominated personnel will be maintained by the Data Protection Officer

For the purposes of this policy the term "Database" refers to a structured collection of records or data held electronically which contains person identifiable information. In the event that further guidance is needed in respect to what constitutes a database please contact the Data Protection Officer.

1.1. Back-ups

Backups will be conducted by Cornwall IT Services. The process and schedule will be documented and made available to those staff within CITS with Backup responsibilities.

1.2. Disclosure of Information

It is important that information about identifiable individuals (such as the general public, patients and/or staff) should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations.

Some disclosures of information may occur because there is a statutory requirement upon RCHT to disclose e.g. with a Court Order, because other legislation requires disclosure (for staff to the tax office, pension agency and for patients to the Department of Health if the patient has a notifiable disease).

Please refer to the Policy to Manage Information and Records,. Access to and Disclosure of Personal Identifiable Data.

Disclosure and use of personal information, whether it be directly identifiable or through the use of other information systems must only be done in accordance with Trust needs following appropriate approvals.

No Trust data should be processed for personal purpose, this includes:

- Access to staff members own records

- Access to family or friends records without legitimate work based relationship being established. i.e. there must be a Trust approved purpose for access.
- Further processing of Trust data for personal gain. No data shall be used for commercial activities whether for financial gain or as part of non-trust approved activities.

1.3. Information in Transit

If person identifiable information/records need to be transported in any media such as: disc, memory stick or manual paper records, this should be carried out to maintain strict security and confidentiality of this information. For further information transporting, sending and receiving person identifiable information please refer to RCHT IT Security, Policy to Manage Information and Records and Email Policy.

1.4. Subject Access Requests

Current Data Protection legislation allows an individual who is the subject of personal information processed by RCHT to access their information. In the event that an individual wishes to have a copy of their information under the subject access provision of the Data Protection Act a request must be made in writing to the Disclosure Office.

RCHT is obliged to respond to requests promptly within 40 days of a request being made for access to records containing person identifiable information. Failure to do so is a breach of the Act and could lead to a complaint to the Information Commissioner. If it is anticipated that a request will take longer than the 40-day period, RCHT will inform the applicant giving an explanation of the delay and agree a new deadline.

In addition, RCHT will charge for any subject access requests made in line with legislative guidelines.

Please refer to the Policy to Manage Information and Records, Appendix 5. Access to and Disclosure of Personal Identifiable Data.

1.5. Disclosure of Information outside the EEA

Personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the European Economic Area to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

In the event that any member of staff wishes to process personal information outside of the United Kingdom, then the Head of Corporate Compliance must be consulted prior to any agreement to transfer or process information.

1.6. Training

The Head of corporate Compliance has overall responsibility for maintaining awareness of confidentiality and security issues for all staff. This is carried out at

regular training sessions covering the following subjects:

- Personal responsibilities
- Confidentiality of personal information
- Compliance with the Data Protection Principles
- Registration of automated databases
- Individuals rights (access to information and compliance with the principles)
- General good practice guidelines covering security and confidentiality
- Contact information relating to who is the Data Protection Officer and how they can be contacted for all problems which may occur in the areas of security and confidentiality of personal information
- Details on patient's rights not to allow us to share their information with other organisations.
- Sealed Envelopes.
- A general overview of all Information Governance components
- General common sense issues such as locking doors and avoiding gossip in open areas
- Letting all staff know about relevant policies, procedures and good practice guidance and where this can be found
- A brief overview of how the data protection and freedom of information acts work and the differences

1.7. Induction

All new starters to RCHT will be given Information Governance training, which will include compliance with the Data Protection Act and general IT security training, as part of the induction process. Extra training in these areas will be given to those who need it such as application/systems managers and those dealing with requests for information. A register will be maintained of all staff attendance at training sessions. Non-contract staff and those on short fixed term contracts will also be required to attend induction sessions. These people will include temporary, agency staff and student placements.

All staff will be made aware of what could be classed as an information security incident or breach of confidentiality. They will be made aware of the process to follow and the forms to complete, so that incidents can be identified, reported, monitored and investigated.

1.8. Contracts of Employment

Staff contracts of employment are created and monitored by RCHT Human Resources department. All contracts of employment include a data protection and general confidentiality clause. Agency and non-contract staff working on behalf of RCHT will be subject to the same rules.

Contractors and Visitors will be required to sign a confidentiality agreement prior to commencing their activities within the Hospital boundaries

All RCHT employees accessing electronic systems will be made aware of their responsibilities in connection with the Acts mentioned in this Policy through a sign up process prior to being given access to systems.

1.9. Disciplinary

A breach of the Data Protection principles could result in a member of staff facing disciplinary action. A copy of RCHT's Disciplinary Procedure is available via the online Document Library.

2. Disclosure of Personal Information

There are Acts of Parliament that govern the disclosure of personal information. Some of these Acts make it a legal requirement to disclose and others that state that information cannot be disclosed.

These include:

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS SHAs from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976
- Gender Reassignment Act 2004

2.1. Obtaining Consent

The RCHT will ensure that the general public, staff, including volunteers, locums, temporary employees and patients are aware of why the NHS needs information about them, how this is used and to whom it may be disclosed by the use of leaflets, posters and the RCHT web site.

2.2. Disclosure to the Police

In almost every case the Police will need to have made the appropriate application for information through the Disclosure Department. The request should be made in accordance with Section 29 of the Data Protection Act 1998, this allows access for:

(a)the prevention or detection of crime,

(b)the apprehension or prosecution of offenders, or

(c)the assessment or collection of any tax or duty or of any imposition of a similar nature,

In most cases the data subject should be informed that the information has been disclosed to the police, unless by doing so any legal and formal investigation would be jeopardised.

The Head of Corporate Compliance is the trust Data Protection Officer and will have the authority to disclose information as is deemed appropriate, or withhold information if the request does not have the necessary substance within the DPA to do so.

Any requests for information that are for the investigation of a serious crime such as: sexual assault, gun or knife injuries, murder, Road Traffic Accident, unexplained

death or Terrorism should be disclosed and can be done so by a senior manager within the Trust.

2.3. Data Protection Principles

There are eight principles of good practice within the Data Protection Act 1998. This is normally referred to as the 'Data Protection Principles'.

Principle 1 Personal data shall be processed fairly and lawfully

There is a requirement to make the general public who may use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. All processing of data should be consistent with the principles of this Act.

Principle 2 Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Information that is processed must only be done so for its intended purpose or purposes. These purposes are shown on the Trust's Fair Processing Notices which are displayed around the Trust.

No personal data should be further processed without the explicit consent of the data subject or in compliance with current legislation.

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

Information collected from individuals should be complete and should be justified as being required for the purpose it is being requested. If the information is not used it should not be collected, unless it is to ensure compliance with statutory obligations.

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

Data must where practicable be accurate and up to date. The Trust should take all steps possible to ensure data is checked for accuracy. This will include Receptionist and Ward clerks checking at every attendance if patient information is accurate. At minimum this should include:

- Name
- Address
- Post code
- GP Details

Ideally this should also include:

- Next of Kin
- Religion
- Ethnicity
- Disabilities
- Preferred method of communication.

Principle 5 Personal data processed for any purpose of purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The Trust has a Retention and Destruction strategy which is part of the Policy to Manage Information and Records Policy which can be found of the Document library.

Principle 6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

Individual's rights – including subject access/right to complain.
Under this principle of the Data Protection Act individuals have the following rights:

- Right of subject access
- Right to prevent processing likely to cause harm or distress
- Right to prevent processing for the purposes of direct marketing
- Right in relation to automated decision taking
- Right to take action for compensation if the individual suffers damage
- Right to take action to rectify, block, erase or destroy inaccurate data
- 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.

Principle 7: Data Security - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

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.
These include:

- All laptops to be encrypted
- USB Sticks must be Trust approved (encrypted devices)
- No personal data to be stored on the Hard drive (C Drive) of desktop devices.

Measures will be taken to ensure that:

- All software and data is removed from redundant hardware and media storage (before the hardware is removed from the Trust.
- Confidential paper waste is shredded or is collected and held in a secure area prior to shredding/incinerating.

Principle 8 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.

If staff are required to send personal identifiable information in a computer readable format to a country outside of the EU, this must not be done without the specific agreement of the Trust Data Protection Officer/Caldicott Guardian, as levels of protection for such information may not be as comprehensive as those in the UK. Similar safeguards must be taken for manual records.

3. Monitoring compliance and effectiveness

Element to be monitored	Trust adherence with the principles of the Data Protection Act 1998
Lead	Head of Corporate Compliance
Tool	Datix Incident & Risk Management Tool
Frequency	There is a need to regularly report on Data Protection issues to the Information Governance Committee. This will require a quarterly reporting cycle.
Reporting arrangements	The full report will be submitted to the Information Governance Committee for interrogation and approval of recommended actions. Any such report will be documented in the minutes of the Information Governance Committee. The chair will delegate any required actions and a relevant timescale for completion. The IGC reports to the Trust Board via the Governance Committee
Acting on recommendations and Lead(s)	The Information Governance Lead/Data Protection Officer will take the lead for ensuring that subsequent recommendations are acted on, working with the Caldicott Guardian and appropriate senior managers to ensure that relevant action plans are put in place for any or all deficiencies and recommendations within reasonable timeframes.

Appendix 2. Freedom of Information

1.1. Publication Scheme

The Trust's Publication Scheme is available on the Trust website. Applicants who require information from the Publication Scheme may download documents from the website or make a written request for a hard copy to be posted to them.

1.2. Rights of Individual Access

There is a requirement to provide a substantive response to any request for information promptly and in any event within 20 working days. There is some scope to extend this timescale if a qualified exemption is being considered and it is necessary to assess the balance of public interest. Further guidance is available from the Information Commissioner's website.

1.3. What information is subject to the Freedom of Information Act?

All recorded information held by, or on behalf of, a public authority is within the scope of the Act (although the disclosure of personal data is subject to the Data Protection Act (DPA) and the Access to Health Records Act (AHRA)). The legislation applies regardless of the age, format, origin or classification of information. It covers files, letters, databases, loose reports, emails, office notebooks, videos, photographs, etc. It extends to closed files and archived material as well as information in current use

1.4. Identifying and recording a Freedom of Information Act request

Any correspondence could include a request for information, so long as it is in writing (including email), gives the name and address of the applicant, and

describes the information requested. The correspondence does not need to mention the FOIA.

In theory this definition would encompass almost all written requests for information received by the Trust, but for pragmatic reasons, where information is given out as part of normal business practice it does not need to be managed (logged and tracked).

Other requests do not need to be managed under the FOIA, where the information is:

- Already accessible e.g. via Publication Scheme or from other organisations;
- Requested by organisations with whom the Trust has a data sharing protocol;
- Not requested in writing.

Requests will be managed under the FOIA if they meet any of the following criteria:

- Are received in writing, print or electronic, giving a name and contact address and would not be regarded as normal business;
- It is likely that the requested information cannot be disclosed (as described within Trust policy on complying with the Data Protection Act);
- Complying would exceed the limit in the Fees Regulations (currently £450);
- The request could not be met within the 20 working day deadline;
- Following a search it is found that no information is held;
- Further information is required from the applicant in order to identify the information.

Within a maximum of three working days, the recipient (which may be any member of staff) of a written request for information must assess it against these criteria, to establish whether it needs be formally managed as an FOIA request and if so, forward the details of the request to the Information Governance Team. (email: rch-tr.foi@nhs.net)

Even if written requests do not need to be formally managed as FOIA requests, all staff should ensure that any requested information is provided within 20 working days. The clock starts the day after the Trust receives the request. A request is considered to be “received” when it is delivered to the Trust or when it is delivered to the email inbox of a member of staff. The date of receipt is not the date the request was passed to the appropriate person for processing.

All managed requests will be logged by the Information Governance Team.

1.5. Responding to a request

Upon receipt

Upon receipt the FOIA request should be referred immediately to the FOI Officer who will respond within 2 working days to inform the applicant that their request has been received and is being processed. The FOI Officer will liaise with the appropriate member(s) of staff, where relevant, to draft a response to the request, and will log the request.

If the FOI Officer has sufficient information to respond to the request, they will inform the applicant in the acknowledgement that their request will be processed within a maximum of 20 working days. They will inform the applicant in writing of any charges, if known, and that no information will be provided unless the charge is paid within three months. This will constitute the issue of a Fees Notice, as described in Section 9 of the FOIA. The Publication Scheme will make clear whether there will be any charges for the information provided through that mechanism.

If the applicant has not provided sufficient information for the request to be processed the FOI Officer will contact the applicant to request the information required before passing the request on to the Designated Respondent. The FOI Officer will ensure that the request is logged on the database and pass the request to the appropriate department for a response to the request.

If there is evidence to demonstrate that the request is vexatious or repeated as defined under Section 14 of the FOIA then the request is to be referred to the Freedom of Information Lead.

Providing the information

If no exemptions or charges are applicable, the information requested by the applicant will be provided within 20 working days. Information that should be provided to applicants is:

- A copy of the information in permanent form or another form acceptable to the applicant ;
- Provision of a digest or summary in permanent form or in another form acceptable to the applicant.

It is not necessary to create new information in order to answer a request, even if this can easily be done from other information that is held, however, it is reasonable to expect that if the information is held it will be provided in the format requested if this can be achieved within the time and cost limits detailed in the FOIA.

Round-Robin Requests. Round-robin requests, as defined above, must be treated in the same way as any other FOIA request; the fact that the requestor has asked other similar public bodies for the same information should make no difference to how the Trust responds.

1.6. Applying exemptions and the public interest test

Exemptions are divided into two categories:

- Absolute. The Trust is not required to disclose the information.
- Qualified. The Trust must apply a public interest test, considering whether the public interest in disclosure outweighs the public interest in non-disclosure. If the public interest does outweigh disclosure, then the information should be disclosed anyway.

When implementing this procedure, the FOI Officer will identify when exemptions

need to be applied and who should be involved in the decision making process, depending upon the circumstances of the particular case. If exemptions are being considered, there should be consideration of potential media interest. Approval from the Chief Executive may be required for decisions on the application of exemptions and the public interest test.

1.7. Refusal to disclose

A refusal of a request may apply to all, or part of, the information requested by an applicant. A request for information may be refused if:

- The Trust considers the information to be exempt from disclosure;
- A charge has not been paid within three months beginning on the day on which the applicant was informed of the charge;
- The cost of compliance exceeds the limit (currently set at £450);
- The request is demonstrably repeated or vexatious.

Notifying the applicant of a refusal of request

If the Trust decides to refuse a request for information under any of the above clauses, the FOI Officer must inform the applicant in writing of the reason why, within 20 working days.

If the reason is because the information is exempt, the notification should state that an exemption applies and why. In addition, in the case of a qualified exemption, the notification should state why it is in the public interest to withhold the information requested. At the same time the applicant should be informed that they can request a review of the decision to deny disclosure and of their right to complain to the Information Commissioner. Reviews are undertaken by the FOI Lead, or via other local arrangements.

1.8. Complaints

Where a decision has been made to refuse to disclose information requested or the requestor is not content with the information that has been provided under the FOIA the applicant can take their case directly to the Information Commissioner for review. However, they should also be offered the opportunity to have the Trust's response reviewed by the Trust. The process detailed below also relates to complaints received regarding the Trust's Publication Scheme.

Internal Review.

If the requestor wishes to instigate an internal review of the response that they received from the Trust they are to do so by either writing or sending an email to the FOI Officer. Internal reviews should be completed within 20 working days of the request being received but this time limit may be extended in exceptional circumstances. The FOI Officer will then inform the Communications Manager by email that an Internal Review has been requested quoting the original request Datix reference.

1.9. The FOI Officer will.

- Open a new FOI request in the database and cross-refer this new request to the original request.

- Contact the person that provided the response (the designated respondent) to the original request to inform them that an internal review has been requested.
- Ask the designated respondent to compile a file containing a complete audit trail of the information gathered by them when generating their response to the request.
- Ensure the designated respondent and FOI Lead are aware that the response to the Internal Review should be completed within 20 working days.

The FOI Lead will carry out the internal review and communicate the results of the review directly with the requestor. The FOI Lead must remain impartial throughout the FOI response process in order to carry out the role of reviewing the Trust's responses to FOI requests. In the event that the FOI Lead has been involved in the initial response to the request that is now subject to internal review then the role of independent adjudicator will be performed by the Corporate Secretary.

The FOI request logged on the Datix system as a result of this process will be closed when the FOI Lead informs the FOI Officer that the internal review process has been completed.

External Review.

Requestors can proceed directly to an external review of their case without using the Trust's internal review process or if they are not content with the results of the Trust's internal review. In either case the final arbiter of complaints relating to FOIA responses is the Information Commissioner's office and complainants should be advised to contact the Information Commissioner's office directly.

1.10. Implications for the Trust

The timescales for responding to FOIA requests are relatively short, and if they are to be met, information will need to be readily accessible. Non-transitory emails should be stored in the same way as other electronic documents.

When creating any written document (including emails), staff should bear in mind that it is liable to be disclosed under the FOIA unless the entire content is exempt. Where part of a document is exempt, but the remainder is not, a redacted version (i.e. a copy with the exempt parts removed) must be supplied to the person requesting it.

Staff should refer any FOIA requests which they may receive promptly to the FOI Officer.

1.11. Training and Support

The Trust will provide appropriate training to all staff on information governance, and specific requirements are addressed within individual policies where applicable. Managers and other staff may request advice from the FOI Lead should they require support with the implementation of this policy.

1.12. Environmental Information requests.

Although this is a different regime, the principles of how this will be accomplished by the Information Governance Team are consistent with that for FOI requests.
Information made available through EIR is that that has a direct effect on the environment, e.g. air, water, earth.
The Trust has a maximum of 20 days to respond to EIR requests, these requests can be either in writing or verbal (differs from FOI where it needs to be in writing).

2. Monitoring compliance and effectiveness

The FOI Officer acts as the single point of contact for all FOIA issues and so they will ensure that responses to requests conform to this policy and remain consistent with the Trust's corporate communications. In addition, adherence to this policy will be audited as part of the routine audit schedule conducted by Internal Audit.

Element to be monitored	Compliance with the requirements of the Freedom of Information Act 2000 & Environmental Information regulations including: a) 20 working day response b) Publication and maintenance of the Trust's Publication Scheme c) Information Commissioner complaints d) Requestor and subject trends
Lead	Head of Corporate Compliance
Tool	Datix FOI application tracks the status of all requests.
Frequency	The Head of Corporate Compliance will provide a report for the Information Governance Committee against elements to be monitored on a monthly and quarterly basis.
Reporting arrangements	Monthly (verbal) and quarterly (written) reports will be presented to the Information Governance Committee who will consider governance or risk issues appropriate for referral to the Trust's Audit Committee.
Acting on recommendations and Lead(s)	Recommendations from the Information Governance Committee will be actioned by the Head of Corporate Compliance and/or the Associate Director of Communications.
Change in practice and lessons to be shared	Required changes to practice will be identified and actioned within 6 months. The Head of Corporate Compliance will be responsible for implementation. Lessons will be shared with all the relevant stakeholders

Appendix 3. Pseudonymisation

1. Business Process

The NHS has used safe havens for over 20 years to ensure the secure transfer of PID. The Trust's Safe Haven Policy provides the guidance regarding the security of transferring information via staff delivery, fax, Email, post and telephone.

All business processes within the Trust must be documented. Business processes can include, but are not limited to:

- the process of using patient data for primary uses
- the process for using patient data for secondary uses
- the use of PID for a combination of primary and secondary

The business process for primary use includes, but is not restricted to; appointment bookings, management of waiting lists or inputting test results. At this stage there is a heightened importance on the accuracy and timeliness of the data. All information recorded about a patient should be recorded in line with the Trust's Clinical Record Keeping Policy, Policy to Manage Information and Records, and the Data Protection Act 1998.

Secondary use business processes must be undertaken with de-identified data. Any processes that are using PID must be modified in line with this policy. If the business process requires confirmation that the patient is registered within a GP practice within the Trust's area this can be identified via the New Safe Haven route.

All business processes must be regularly reviewed to monitor the impact of de-identifying the data. Within the review the New Safe Haven route should be monitored if a piece of PID is a requirement of the analysis, for example postcode may be required if a geographical outcome is to be achieved.

1.1. De –Identification

Staff only has access to the data that is necessary for the completion of the business activity for which they are involved in. This is reflected in Caldicott Principles; access should be on a need to know basis. This principle applies to the use of PID for secondary or non-direct care purposes. By de-identification users are able to make use of patient data for a range of secondary purposes without having to access the identifiable data items.

The aim of de-identification is to obscure the identifier data items within the patient records sufficiently that the risk of potential identification of the subject of a patient record is minimised to acceptable levels, this will provide effective anonymisation. Although the risk of identification cannot be fully removed this can be minimised with the use of multiple pseudonyms.

De-identified data should still be used within a secure environment with staff access on a need to know basis.

De-identification can be achieved by:

- Removing patient identifiers. (Name, Date of Birth etc.)
- The use of the identifier for example; value ranges instead of age.
- By using a pseudonym. (a unique index number only relating to that patient)

When Pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual patients across different data sets and over time. This allows the linking of data sets and other information which is not available if the PID is removed completely.

If patient data is required the NHS Number is the most secure form of identifiable data. The NHS Number should be included within all patient records and documentation in line with the current Connecting for Health NHS Number Campaign.

1.2. Pseudonymisation

To effectively pseudonymise

data the following actions must be taken:

- Each field of PID must have a unique pseudonym.
- Pseudonyms to be used in place of NHS Numbers and other fields that are to be used by staff must be of the same length and formatted on output to ensure readability. For example, in order to replace NHS Numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers.
- Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports.
- Pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised.
- The secondary use output must only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines.
- Pseudonymised data should have the same security as PID.

Use of Identifiable Data

If PID data is required or there is a need to de-pseudonymised data the reasons and usage of the data should be fully documented and approval is required by the appropriate data owner. This auditable trail of access to patient's records supports the Care Record Guarantee where patients are to be informed as to who has accessed/seen their data and the audit will provide accurate data in the event of untoward incidents.

The key items to be documented are:

- Who has accessed each data base containing identifiable data.
- Date and time of access. (unless legacy systems do not support this)
- The reason for the access. (unless legacy systems do not support this)
- The output from the access. (unless legacy systems do not support this)

This audit should be kept within a separate structured database to enable queries and audit.
The log of accesses must be regularly audited via sampling of users or subject matter to check for unusual patterns of access.

1.3. Transferring Information

Appropriate data sharing agreements should be in place when information is to be transferred to another organisation. The Information Sharing Protocol should be signed by the organisations Caldicott Guardian or delegated authority. The Agreement should be produced in line with the Data Protection Act 1998 and Caldicott Guidelines.

If the transfer of information is required for secondary use a form of pseudonymised data should be sent.

2.1. Data Transfers

The Trust must identify all flows of PID both internal and external. Any risks identified must be reported in line with the IG Toolkit requirements and measures put in place to reduce the risk. This links with the IG Toolkit, this must be at a level 2 in line with the Trust's Statement of Compliance.

There should also be a more detailed information flow which shows all of the data flows from primary use systems to enable secondary use. Primary use systems could include patient administration systems including PAS, Maxims, Galaxy etc. These flows should be electronic only; via system to system transfer or via email. If the data flows show that information is transferred in a paper based format, even if used Safe Haven methods, this should cease to ensure a more secure and encrypted transfer of data. However until full electronic transfer is available the Trust's Safe Haven Policy should be adhered to regarding paper based data flows.

2.2. Information Asset Register

The Trust must identify who has access to identifiable data for purposes of allowing access to identifiable data, together with the reasons for their access. This also provides the means of being clear about who should not have access to identifiable data. This links into the IG Toolkit, this must be at a level 2 in line with the Trust's Statement of Compliance.

2.3. Smartcard access

The Trust must put in place processes to vet, register and authorise the users of identifiable and pseudonymised data. This links into the IG Toolkit requirements; this must be at a level 2 in line with the Trust's Statement of Compliance. The implementation RA arrangements fall under the remit of the RA Manager who is part of Cornwall IT Services. Please refer to the Trust's Integrated Identity Management Policy for further details about the use of smartcards and various roles within the organisation.

2.4. Access Control Facilities

End user applications that provide patient level data must be modified to enable separate views of pseudonymised and identifiable data. The applications will also need to interact with the access control facilities. Information Asset Owners (IAO) should implement appropriate access control functionality for assets under their control in line with the Trust's Risk Management Strategy. Access will only be provided to individuals who have been duly authorised by the IAO and ensure appropriate technical functionality and management controls exist to support and maintain this.

2.5. Audit

There must be an access log maintained in relation to PID, which should enable auditing of the access to identifiable data by individual users. The logging and audit facilities are required to ensure that only appropriate access to identifiable data has been undertaken and to support the Care Record Guarantee.

In accordance with the IG Toolkit requirements these access logs must be regularly monitored

3. Monitoring compliance and effectiveness

3.1. There must be an access log maintained in relation to those with access to the New Safe Haven. This will enable auditing of the access to identifiable data by individual users. The logging and audit facilities are required to ensure that only appropriate access to identifiable data has been undertaken and to support the Care Record Guarantee.

3.2. In accordance with the IG Toolkit requirement these access logs must be regularly monitored to ensure

- the correct staff members are accessing the PID
- that it is being accessed for limited purposes
- to check for unusual patterns of access. If any unusual patterns of access are noted this will be reported via the Governance Committee.

3.3. The New Safe Haven route will be reviewed routinely to ensure that the principles of pseudonymisation are being upheld

Element to be monitored	Access to the new safe haven via SharePoint application
Lead	The Information Services Manager and the Information Governance Manager
Tool	The security model for the SharePoint (new safe haven) solution will be used as a log of all Users. This lists all users and their access to folders enabling monitoring of numbers of users and levels of access. A log is also created that shows the specific files that users have been accessing. This allows monitoring of how much patient identifiable information is being accessed and by whom

Frequency	Usage will be monitored on a monthly basis. If the usage report reflects a cause for concern a full report will be produced with immediate effect. The report will include investigations that have taken place and recommendations for actions to be taken.
Reporting arrangements	The full report will be submitted to the Information Governance Committee for interrogation and approval of recommended actions. Any such report will be documented in the minutes of the Information governance committee. The chair will delegate any required actions and a relevant timescale for completion.
Acting on recommendations and Lead(s)	The Information Governance Manager will take the lead for ensuring that subsequent recommendations are acted on, working with the Information Services manager to ensure that relevant action plans are put in place for any or all deficiencies and recommendations within reasonable timeframes.
Change in practice and lessons to be shared	Required changes to practice will be identified and actioned within four weeks. A lead member of the team will be identified to take each change forward where appropriate. Lessons will be shared with all the relevant stakeholders.

Appendix 4. Information Governance Policy

1 Standards and Practice

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely, and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians, managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

There are 5 key interlinked strands to the IG policy:

- Openness
- Legal compliance
- Information security
- Quality assurance
- Training and awareness

1.1. Openness

- Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlines in the Data Protection Act. Non-confidential information on the Trust and its services should be available to the public through a variety of media, in line with the Trust's code of openness.

- The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act.

- Patients should have ready access to information relating to their own health care, their options for treatment, and their rights as patients. There will be clear procedures and arrangements for handling queries form patients and the public.

- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

- The Trust regards all identifiable personal information relating to persons as confidential, compliance with legal and regulatory framework will be achieved, monitored and maintained.

- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

- IG training including awareness and understanding of Caldicott principles and confidentiality, information security, FOI and data protection will be mandatory training on an annual basis for all staff. IG will be included in induction training for all new staff. The necessity and frequency of any further training will be appraisal based.

- All projects involving significant change or implementation of new data processing must have a Privacy Impact Assessment conducted prior to go-live.

1.2. Legal Compliance

- The Trust regards all identifiable personal information relating to patients as confidential.

- The Trust will undertake or commission annual assessments and audits of its compliance with IG requirements.

- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Access to Health Records Act, Human Rights Act, The Public Records Act 1958 and the common law confidentiality.

- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

- The Trust has a comprehensive range of policies supporting the information governance agenda which can be found on the Trusts Document Library, this is accessible via the Intranet or the Internet.

1.3. Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.

- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.

- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures, and training.

- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

1.4. Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of all records.

- The Trust will undertake or commission annual assessments and audits of its information quality and all records management arrangements.

- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

- Wherever possible, information quality should be assured at the point of collection.

- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training

1.5. Training and awareness

- IG is part of induction training. All new staff will receive awareness training and information on information governance, which will include Caldicott and confidentiality, data protection, information security and Freedom of Information.

- IG Training forms part of the Trusts suite of mandatory training requirements. The courses are available on NLMS.

Appendix 5 Safe Haven Policy

1.1 Introduction

All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of the personal information held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive information.

The NHS has used safe havens for over 20 years to ensure the safety and secure handling of confidential patient identifiable information. The first use was to provide security when faxes were used to transmit patient data between providers and

purchasers. Where other Trust locations, other Trusts, or other agencies want to send personal information to a Trust department, they should be confident that they are sending to a location which ensures the security of the data.

The Safe Haven model continues to develop with the inclusion of the New Safe Haven concept. Under the obligations of Pseudonymisation the restriction of access to identifiable data is expanded to support the process that enables de-identified records to be created, hence the term New Safe Haven.

This version supersedes any previous versions of this document.

1.2 Purpose of this Policy

The aim of this policy is to ensure that the use of person information is subject to the same strict controls, which already apply elsewhere, where confidential information is handled. There is a requirement to reassure patients, staff and the public that information will be handled securely and safeguards are in place to ensure its security.

1.3 These safeguards include:

- Fax machines located in a secure room or cupboard.
- A directory of Safe Haven fax machines.
- Provision of patient identifiable information for primary purposes only
- De-identification of patient identifiable information
- Anonymisation of patient identifiable information
- Pseudonymisation of patient identifiable information

2.2 This policy provides:

- Information relating to the legislation and guidance which dictates the need for a safe haven and a new safe haven
- A definition of the term ‘safe haven’ and also of ‘new safe haven’
- The circumstances under which a safe haven/new safe haven are required
- Established processes and accountability to ensure that the identity of patients is protected when their information is used for secondary purposes
- The necessary procedures and requirements that are needed to implement a safe haven or a new safe haven
- Identification of those who are able to access the safe haven/new safe haven and those to whom disclosure can be made
- The circumstances under which patient identifiable information can be accessed
- Clarity to staff, managers and contractors about their responsibilities and the limits to which they can or cannot access identifiable patient information

A number of Acts and department of health guidance dictate the need for safe haven arrangements to be established, they include:

- **Data Protection Act 1998**

Principle 3 states that “personal data will be adequate, relevant, and not excessive”. This is relevant for fax transmissions which should only include the relevant personal information that the recipient needs to know. For patient information, in many cases the NHS Number, PAS number and/or postcode are sufficient and the patients’ name may not need to be included.

Principle 7: “Appropriate technical and organisational measures shall be taken to make personal data secure”

- **NHS Code of Practice: Confidentiality**
  Annex A1 Protect patient Information “Care must be taken, particularly with confidential clinical information , to ensure that the means of transferring from one location to another are secure as they can be”

- **Care Record Guarantee**
  Details 12 commitments we make to patients. These cover how we internally control and manage data, with whom we share it, and what actions we will take if we identify inappropriate access.

- **Common Law duties of confidentiality**
  All patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.

We will only disclose information in the following circumstances.

- where the individual to whom the information relates has consented;
- where disclosure is in the public interest; and
- where there is a legal duty to do so, for example a court order

- **Pseudonymisation Requirements**

As detailed in Reference Paper 2: ‘Guidance on Business Processes and New Safe Havens Final v1.0-20 November 2009

2. Scope

This policy is concerned with the security of patient information and is relevant to all staff groups who have access to patient level information for both primary and secondary purposes.

The traditional concept of a Safe Haven relates to a location where personal information is being received held or communicated, especially where the personal information is of sensitive in nature e.g. patient-identifiable information. There should be at least one area designated as a safe haven at each of the Trust sites. Safe Haven procedures should be in place in any relevant location.

The concept of the Safe Haven continues but is now supplemented by the role of the New Safe Haven.

The New Safe Haven comprises elements that are virtual in nature as well as certain teams and individuals. The virtual element, represented by the Business Intelligence Data Warehouse will be implemented by the Information Services Department. Key roles will be played by members of the shared information technology service (CITS) and the Finance PLiCS team.

This Policy will be reviewed in line with the policy on policies by the Information Governance Committee. Throughout the Pseudonymisation Project and beyond to include business as usual practices this policy will be reviewed by the Information Governance Manager in line with any new guidance or changes within procedure.

3. Standards and Practice

4. Requirements for Safe Havens

Location/security arrangements (Physical)

- It should be a room that is locked or accessible via a coded key pad known only to authorised staff or
- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any member of staff who work in the same building or office, or any visitors.
- If sited on the ground floor any windows should have locks on them.
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Manual paper records containing person identifiable information should be stored in locked cabinets.
- Computers should be not left on, in view or accessible to unauthorised staff, have a
- Password access and secure screen saver function
- Equipment should be switched off when not in use.

4.2 Fax Machines

There should only be one fax machine used to transmit or receive person identifiable information in each clinical or managerial unit. This should be a Safe Haven fax. This fax number should be known as the only number available specifically for the purpose of receiving confidential personal information for the unit. The Safe Haven fax machine should be kept in a secure location with only authorised personnel gaining access to the room and its facilities. If a securely locked room is not available, then the fax machine should be kept in a secure room away from patients and none departmental staff.

The Trust is moving towards replacing physical fax machines with an electronic process which mirrors the use of the current machines. This will allow electronic documents to be received (RCHT only) into secure folders on servers, rather than relying on paper copies. This will ensure extra security of documents and will strengthen the rigor of accurate and timely facsimile transfers.

The following rules must apply when sending a fax:

- You must ensure the fax number to be used is the correct one.
- Care is taken in dialling the correct number.
- Numbers in regular use should be stored in the memory of the machine to reduce the risk of error when entering the number.
- The sender must be certain that the intended recipient will be available to receive the fax at the other end and confirm receipt.
- Confidential faxes must not be left lying around for unauthorised staff to see.
- Only the minimum amount of personal information should be sent, where possible the data should be anonymised or a unique identifier used.
- Fax should only be sent to a safe location where only staff that have a legitimate right to view the information can access it.
- Fax machines must only be used to transfer personal information where it is absolutely necessary to do so.

Faxes including person identifiable information must have a top sheet of paper to be sent through the machine first stating:

- Who the fax is from
- The name of the recipient
- The number of pages the fax contains (including the top copy)
- Notification for the recipient to contact the sender on the arrival of a fax
- The following Confidentiality Notice must be included on the top copy of all faxes relating to patient information that is sent out:

The information contained in this fax is STRICTLY CONFIDENTIAL and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately.
Thank you.

4.3 Misdirected Faxes

Information received in a misdirected fax should be treated as highly confidential and should not be divulged to others.

- A misdirected fax can be received from both internal or external sources, and needs to be treated as a sensitive document.
- Staff must be made aware of the requirement to notify the sender of misdirected faxes, and must treat the contents in an appropriate manner.

4.4 Receiving Unsolicited Faxes

Unsolicited or unexpected faxes should be treated with care until the sender has been identified.

- Faxes that look official can lead to the disclosure of confidential information.
- Responding to unsolicited faxes may encourage further faxes from the same source. This could be part of a plan by an opportunist hacker probing the area for information to find security holes.
- Staff must be made aware of requirement to safeguard Safe Haven faxes.

4.5 Communications by post

Care should be taken when transferring information by post.

- Outgoing mail (both internal and external) should be sealed securely and marked private and confidential
- Any mail that appears to be incorrectly sealed must be returned to the source.
- Any mail that appears to be poorly addressed must be returned to the source.
- If the post room staff have any cause for concern relating to the confidentiality of the post, they should escalate their concerns to their line manager. They should not attempt to open the mail.
- It should be clearly addressed to a named recipient or department role.
- An assessment must be made as to the method of posting, if it is confidential information that can identify an individual, it should be sent recorded delivery.
- Permission must be sought for sending sensitive clinical information by post, unless it is an agreed and accepted business practice. E.g. Discharge Summary to a GP.

4.6 Computers

- Access to any PC must be password protected, this must not be shared.
- Computer screens must not be left on view so members of the general public or staff who do not a justified need to view the information can see personal data. PCs or laptops not in use should be switched off or have a secure screen saver device in use.
- Information should be held on the organisation's network servers, not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.
- All personal information sent by e-mail should be protected by adding the following in the subject [secure] (include brackets).
- Personal information of a more sensitive nature should be sent over NHSmail when available. No emails should be sent with confidential contents to Hotmail accounts unless they are encrypted.
- Clinical information is clearly marked
- Emails are sent to the right people (please refer to the Email Policy)
- Browsers are safely set up so that for example, passwords are not saved and temporary internet files are deleted on exit
- Information sent by email will be safely stored and archived as well as being incorporated into patient records
- There is an audit trail to show who did what and when
- There are adequate fall back and fail-safe arrangements
- Information is not saved or copied into any PC or media that is "outside the NHS"
- All laptops must be encrypted by Cornwall IT Services.
- Trust approved encryption USB devises must be used to transfer confidential data.
-

5. Additional Requirements for New Safe Havens

5.1 Data Flows

All flows of patient identifiable information should be logged on the Data Flows Register held by the Information Governance Manager. The data flow register will include intelligence relating to;

- where the data flow originates (ie which system)
- the team or individual responsible for processing the data
- the individuals who have access to the data

All such flows should be risk assessed to ensure that the risk is within the local context of ‘acceptable risk’.

5.2 User Access

All staff members accessing the New Safe Haven will be required to complete an Access form. It is the responsibility of the systems Information Asset Owner or delegated senior manager for their area to counter signed the form.

The default position is that access to patient identifiable information will not be provided to members of staff outside of the direct and indirect care teams described under the glossary section of this policy. Any exceptions should be approved by the Caldicott Guardian, or his nominated delegate (Head of corporate Compliance), who must be satisfied that there is genuine justification in order for an individual to perform their role. All such exceptions should be flagged accordingly on the user register.

Current exceptions (including justification);

- RCHT Information Team: to transfer information from legacy systems such as PAS into the data warehouse environment and to enable Data Quality (DQ) and validation processes to be undertaken.
- Cornwall IT Services Data Quality team: to enable DQ duties to be carried out.
- Cornwall IT Services Database Management Service: to enable production of Commissioning Data Sets and maintenance of the data warehouse.
- Finance Patient Level Information and Costing team: to enable production of patient level/service line reporting to the healthcare team. This will be in a de-identified format.
- Finance Commissioner Invoice liaison: to enable verification of patients specified on invoices to commissioners and ensure that the Trust is paid for all activity. This will be in a de-identified format.
- Information Governance Manager, who has responsibilities for conducting access audits,.

5.3 User Register

All Users approved for access to patient identifiable information held within the New Safe Haven will be entered into the User Register held and maintained by CITS. This will enable audit to be carried out.

All staff movements will be recorded and access levels assessed to ensure the continued need as a primary user.

All leavers will have their access terminated.

5.4 Virtual New Safe Haven

The virtual New Safe Haven will be provided via the SharePoint Business Intelligence and data warehouse functionality. This will be maintained and developed by the RCHT Information team, under the leadership of the Information Services Manager.

The relevant software will be maintained by CITS and reside on a designated server.

The new safe haven functionality will support the de-identification of patient level information as well as the creation of pseudonyms for information provided for a secondary purpose. It will also provide access to information designated as having a primary purpose via an appropriate security model.

5.5 Sharing Information with other Organisations

Employees of the Trust authorised to disclose information to other organisations, either within or outside the NHS, must seek an assurance that these organisations have a designated safe haven point for receiving personal information.

Patient identifiable information should not be sent outside of the NHS unless it is for a primary purpose. In such circumstances information can only be sent from a new safe haven and received by a new safe haven and must be fully encrypted.

The transfer of patient identifiable information, between NHS organisations, for secondary purposes is limited to those purposes published on the Fair Processing Notices. Justification for the need should be easily demonstrable, for example where the Commissioner is required to link up information pertaining to individuals from different systems. In such circumstances information can only be sent from a new safe haven and received by a new safe haven eg from the RCHT new safe haven to the Commissioner new safe haven. In addition the information should be de-identified to include the minimum of identifiers**.**

Where patient activity data is required by the Commissioner (Kernow Commissioning Group) it shall be sent via the DESCRO which will ensure the data is suitably pseudonymised.

The use of this information is limited to those activities that need to take place in order to reconcile the Secondary Uses Service (SUS) submissions to the

Financial/Service Level Agreement (SLA) information. The standard safe haven protocols must be observed.

The Trust must be assured that organisations who will receive such information comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- Data Protection Act 1998
- Common Law Duty of Confidence
- NHS Code of Practice: Confidentiality
- N3 Connectivity.

Staff sharing personal information with other agencies should be aware of protocol agreements with other Healthcare providers and Government organisations. There is an overarching information sharing protocol on the Trusts document library.

6. **Key attributes of the new safe haven**

The NHS has used safe havens for over 20 years to ensure the secure transfer of PID. This Safe Haven Policy provides guidance regarding the security of transferring information via staff delivery, fax, Email, post and telephone and has now been updated to include the New Safe Haven requirement specified under Pseudonymisation.

Under the requirements of Pseudonymisation, a similar concept of restricting access to identifiable data is required to support the process that enables de-identified records to be created, hence the term new safe haven.

The New Safe Haven will provide the means of restricting access to authorised users to identifiable data for secondary purposes and will support de-identification of the identifiable data. It comprises elements that are virtual in nature eg the Business Intelligence Data Warehouse as well as teams and individuals.
This in turn means that:

- Patient information systems and databases must be held within an electronic Safe Haven whereby access is limited and password controlled for each authorised user.
- The facilities can only be used by a small number of authorised staff sufficient to perform the functions and provide cover and back-up to ensure continuity of service
- Authorisation of the staff performing roles in the New Safe Haven should be through the Caldicott Guardian, or his nominated delegate(Information Governance Manager), and the equivalent of local Registration Authority processes for accessing Spine based applications
- Staff will only have access to the data that is necessary for the completion of the business activity in which they are involved. This is reflected in Caldicott Principles; access should be on a need to know basis. This principle applies to the use of PID for secondary or non-direct care purposes.
- The systems (or sub-systems) used for the data transition processes have appropriate access control mechanisms to restrict access to only those

authorised users for the specific purpose of supporting de-identification processes.

- Access to a safe haven will only be given by the Trust's IT Department on the correct completion of the Systems Access Request Change Form.
- A list of the staff able to authorise access to a Safe Haven will be maintained and regularly reviewed by the Information Services Manager.
- A list of the authorised users will be maintained for each safe haven database/system by Cornwall IT Services.
- The New Safe Haven can be defined in terms of
- The activities to be undertaken to support de-identification
- Posts/people authorised to access identifiable data for the purpose of supporting de-identification
- Posts/people authorised to access identifiable data for the purpose of supplying identifiable data to authorised users
- The facilities necessary to support the activities.

The New Safe Haven can also be defined in terms of access control and data management arrangements as these indicate which data can be accessed by what means and by whom.

7. New Safe Haven Security

New safe haven security must conform to NHS good practice concerning the handling of identifiable data. This is particularly important as elements of the new safe haven are virtual in nature and staff members are distributed through the organisation.

In addition;

- Access to safe haven functionality, such as accessing databases for DQ purposes is restricted to registered, authorised users.
- Access to the safe haven functionality is password controlled by individual user accounts and passwords. Accounts must not be shared between users. Password management must meet CfH good practice requirements for strength of passwords, refresh frequency, etc
- Only authorised and registered staff members, have access to the core storage of identifiable and linked data.

8. Monitoring compliance and effectiveness

Element to be monitored	The use of managed permissions for Fax machines, data mapping and software permissions will allow monitoring and management of Safe Haven activities.
Lead	The IG Lead will take a proactive role in monitoring effectiveness of this policy, although others such as the Information Services Manager and Cornwall IT Services play an important role in supporting this.
Tool	Fax machines permissions via CITS, Data mapping and transfers through IG Toolkit submission and meetings where safe haven topics are discussed.
Frequency	IGC meets bi-monthly
Reporting arrangements	The IGC reports to Quality Assurance Coimmittee bi-monthly. Any issues that require senior attention will be raised to the CG or SIRO as required.
Acting on recommendations and Lead(s)	The IGC takes responsibility for identifying, reporting and investigating risks and incidents regarding the IG agenda. The head of IG takes responsibility for ensuring data is transferred and shared appropriately.
Change in practice and lessons to be shared	Required changes to practice will be identified and actioned within the time frame agreed by the IGC. A lead member of the team will be identified to take each change forward where appropriate. Lessons will be shared with all the relevant stakeholders

Appendix 6. Governance sheet

Document Title	Information Use Framework Policy			
Date Issued/Approved:	*28th November 2016*			
Date Valid From:	*28th November 2016*			
Date Valid To:	*28th November 2019*			
Directorate / Department responsible (author/owner):	*Mark Scallan, Head of Corporate Compliance*			
Contact details:	*01872 258580*			
Brief summary of contents	Provides the framework within which the Trust will manage its responsibilities for managing the safe use and sharing of person level data. It also provides detail on how the Trust manages its FOI responsibilities			
Suggested Keywords:	*Use this section to suggest keywords to be added by the Uploader to aid document retrieval.*			
Target Audience	RCHT	PCH	CFT	KCCG
	✓			
Executive Director responsible for Policy:	*Director for Corporate Affairs*			
Date revised:	11 November 2016			
This document replaces (exact title of previous version):	This policy merges the following policies into this one document: Data Protection Policy Freedom of Information Policy Pseudonymisation Policy Information Governance Policy			
Approval route (names of committees)/consultation:	*Information Governance Committee*			
Divisional Manager confirming approval processes				
Name and Post Title of additional signatories	*'Not Required'*			
Name and Signature of Divisional/Directorate Governance Lead confirming approval by specialty and divisional management meetings				
	Name:			

Signature of Executive Director giving approval				
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet & Intranet	✓	Intranet Only	
Document Library Folder/Sub Folder	*Health Informatics / InformationGovernance*			
Links to key external standards	*IG Toolkit* *Data Protection Act* *Freedom of Information Act* *Human Rights Act* *The Environmental Information Regulations 2004* *The Common Law Duty of Confidentiality* *The NHS Confidentiality Code of Practice* *Caldicott 2 Report*			
Related Documents:	*Data Protection Policy* *Freedom of Information Policy* *Pseudonymisation Policy* *Information Governance Policy*			
Training Need Identified?	*No*			

Version Control Table

Date	**Version No**	**Summary of Changes**	**Changes Made by** *(Name and Job Title)*
Jan 2014	*V1.0*	*Initial Issue – merging of* *Data Protection Policy* *Freedom of Information Policy*	*Mark Scallan – Head of Information Governance*
Nov 2016	V2.0	Additional responsibilities identified for all staff Addition of Environmental Information Regulations	*Mark Scallan – Head of Corporate Compliance*

All or part of this document can be released under the Freedom of Information Act 2000

This document is to be retained for 10 years from the date of expiry.

This document is only valid on the day of printing

Controlled Document

This document has been created following the Royal Cornwall Hospitals NHS Trust Policy on Document Production. It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 7. Initial Equality Impact Assessment Form

Information Use Framework Policy – covering safe and legal practices for processing data.	
Directorate and service area: Information Governance	Is this a new or existing Policy? existing
Name of individual completing assessment:	Telephone: 01872 258580
1. Policy Aim* Who is the strategy / policy / proposal / service function aimed at?	The aim of this policy is to establish a consistent and coherent approach to handling Data Protection, data management, confidentiality and Freedom of Information thus ensuring that the Trust can meet its statutory and regulatory obligations.
2. Policy Objectives*	The objectives of this policy is to establish a framework for the Trust in how it will manage its adherence to Data Protection and Freedom of Information legislation and to ensure that procedures are in place for staff to be aware of their responsibilities.
3. Policy – intended Outcomes*	Implementation of this policy will enable the Trust to achieve a high standard compliance with legislation leading to compliance with IGT requirements.
4. *How will you measure the outcome?	Internal Audit will conduct regular audits of all areas of the Trust via a rolling programme of audits.
5. Who is intended to benefit from the policy?	All staff, and service users
6a) Is consultation required with the workforce, equality groups, local interest groups etc. around this policy? b) If yes, have these *groups been consulted? C). Please list any groups who have been consulted about this procedure.	no

7. The Impact Please complete the following table.			
Are there concerns that the policy **could** have differential impact on:			
Equality Strands:	Yes	No	Rationale for Assessment / Existing Evidence
Age	Yes		This policy addresses the management of information and records and takes into account the age of children's records and their respective mother's records when considering data protection

Sex (male, female, trans-gender / gender reassignment)		**No**	There are no sex related aspects to these policies.
Race / Ethnic communities /groups	Yes		The Data protection act covers data processing in relation to race and ethnicity
Disability - Learning disability, physical disability, sensory impairment and mental health problems		**No**	There are no disability related aspects to these policies.
Religion / other beliefs	Yes		The Data protection act covers data processing in relation to religion
Marriage and civil partnership		**No**	There are no marriage or partnership related aspects to these policies,
Pregnancy and maternity		**No**	There are no sex related aspects to these policies,
Sexual Orientation, Bisexual, Gay, heterosexual, Lesbian		**No**	There are no sexual orientation related aspects to these policies,

You will need to continue to a full Equality Impact Assessment if the following have been highlighted:

- You have ticked "Yes" in any column above and
- No consultation or evidence of there being consultation- this excludes any *policies* which have been identified as not requiring consultation**. or**
- Major service redesign or development

8. Please indicate if a full equality analysis is recommended.	**Yes**	***No***

9. If you are not recommending a Full Impact assessment please explain why.

The Framework is designed to support and promote treating all service users with the required considerations under British law.

Signature of policy developer / lead manager / director	Date of completion and submission 11 November 2016

Names and signatures of members carrying out the Screening Assessment	1. Mark Scallan 2.	

Keep one copy and send a copy to the Human Rights, Equality and Inclusion Lead, c/o Royal Cornwall Hospitals NHS Trust, Human Resources Department, Knowledge Spa, Truro, Cornwall, TR1 3HD

A summary of the results will be published on the Trust's web site.

Signed _____

Date _____