Code of Conduct for Employees in Respect of Confidentiality

V2.5

22 September 2014
1. **Introduction**

1.1 All employees working in/with the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998 and, in addition, for health and other professionals through their own professions Code(s) of Conduct.

1.2 For the purposes of this document, the term ‘employee’ is used as a convenience to refer to all those to whom this code of practice should apply. Whilst directed at Trust staff, the Code is also relevant to any one working in and around health. This includes private and voluntary sector staff.

1.3 This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g. business “in confidence” information.

1.4 Disclosures and sharing of personal identifiable information are governed by the requirements of Acts of Parliament and government guidelines.

1.5 The principle behind this Code of Practice (Code) is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Royal Cornwall Hospitals Trust (RCHT) security systems or controls in order to do so.

1.6 This version supersedes any previous versions of this document.

2. **Purpose of this Policy/Procedure**

2.1 This Code has been written to meet the requirements of:

- The Data Protection Act 1998
- The Human Rights Act 1998
- Common law duty of confidentiality
- The Computer Misuse Act 1990
- DoH Confidentiality Code of Practice
- NHS Care Records Guarantee
- Access to Health Records Act 1990
- NHS Records Management Code of Practice
- NHS Code of Practice on Confidentiality
• Caldicott Principles
• Information Use Framework Policy
• Email Policy
• IT Security Policy
• Corporate Information Lifecycle Policy
• Occasional Home Working Policy

2.2. All of the above are available either on the Trusts document library or via the Internet

2.3. This Code has been produced to protect staff by making them aware of correct procedures so that they do not inadvertently breach any of these requirements.

3. Scope
3.1. All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust.

4. Definitions / Glossary
4.1. Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, in whatever format held and stored.

4.2. For example, information may be held on paper, memory stick (flash drives), external hard drives, CD, computer file or printout, video, photograph or even heard by word of mouth.

4.3. It includes information stored on portable devices such as laptops, Tablets, Blackberries, mobile phones, palmtops, USB Flash drives, and digital cameras (this list is not exhaustive)

4.4. It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes any Trust confidential information.

4.5. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, photographs, Videos, Audio Tapes, National Insurance number, IP Address, email address etc.

Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
4.6. Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

4.7. During your work you should consider all information to be sensitive, e.g. staff/patients name and address. The same standards should be applied to all information you come into contact with.

5. **Ownership and Responsibilities**

5.1. Board level responsibility for all matters relating to confidentiality of patients and the ways in which staff conduct themselves in this area comes under the Caldicott Guardian/Medical Director. The wider aspects of confidentiality of personal data which relates to both patients and staff comes under the Head of Information Governance/Data Protection Officer.

5.2. **Role of the Managers**

Line managers are responsible for:

- Ensuring all of their staff have read the policies outlined earlier in this document. (2.1)
- Monitoring their staff to ensure they are acting in ways that support the policies outlined earlier in this document. (2.1)
- Ensuring all their staff undertakes their mandatory annual Information Governance training in line with Trust Policy.

5.3. **Role of the Information Governance Committee**

The IGC is responsible for:

- Monitoring compliance with legislation and Trust Policies through incident reporting.
- Taking any actions that maybe required to mitigate against breaches of confidentiality.
- Members of the Committee can act as a lead investigator where required on data breaches. Reports will also be received by the Committee that relate to data breaches.

5.4. **Role of Individual Staff**

All staff members are responsible for:

- Ensuring they comply with Trust policies, procedure and this Code in order to safely process confidential information.
- To take responsibility for their actions with all regards to confidentiality.
• To report any risks or incidents on the Trusts Incident reporting system Datix.

6. Standards and Practice
6.1. Never give out information about patients or staff to persons who do not "need to know" in order to provide health care, treatment or administrative activities.

6.2. All requests for identifiable information should be on a justified need (as described within the principles of the Caldicott Report) and some may need to be agreed by the Trusts Caldicott Guardian or Data Protection Lead/Head of Information Governance (Appendix A).

6.3. Any exceptions to this rule may require you to get written consent from the patient in advance. If the patient is unconscious and unable to give consent, consult with the health professional in charge of the patient’s care.

6.4. Patients have a right to expect that information about them will be held in confidence by all NHS and health-care staff. Confidentiality is central to trust between health providers and patients. Without assurances about confidentiality, patients may be reluctant to give staff the information they need in order to provide good care. If you are asked to provide information about patients you must:

   6.4.1. be satisfied that patients know about disclosures necessary to provide their care, or for local clinical audit of that care, that they can object to these disclosures but have not done so (use the Care Record Guarantee Leaflet on Information Sharing in discussions with the patient);

   6.4.2. seek patients’ express consent to disclosure of information, where identifiable data is needed for any purpose other than the provision of care or for clinical audit – save in the exceptional circumstances described below;

6.5. You must treat information about patients and clients as confidential and use it only for the purposes for which it was given. As it is impractical to obtain consent every time you need to share information with others, you should ensure that patients and clients understand that some information may be made available to other members of the team involved in the delivery of care. You must guard against breaches of confidentiality by protecting information from improper disclosure at all times.

6.6. You should seek patients’ and clients’ wishes regarding the sharing of information with their family and others. When a patient or client is considered incapable of giving permission, you should consult relevant colleagues. The duty of confidentiality owed to a person under 16 is as great as that owed to any other person. But if the young person or another person, is at risk of serious harm, which disclosure to an appropriate person would prevent, that the need for this will be explained.

6.7. If you are required to disclose information outside the team that will have personal consequences for patients or clients, you must obtain their
consent. If the patient or client withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:

6.7.1. they can be justified in the public interest (usually where disclosure is essential to protect the patient or client or someone else from the risk of significant harm)

6.7.2. they are required by law or by order of a court

6.7.3. Where there is an issue of child protection, you must act at all times in accordance with national and local policies.

6.7.4. Where the disclosure is required for the vital interests of the patient. This is where withholding information would have a significant impact on their life.

6.8. Observe the principle that information given for one purpose may not be used for a different purpose without the permission of the informant;

6.9. Be aware that patients have a right to restrict disclosure of their personal information and as far as possible you must ensure that this right is adhered to and respected. A failure to do so could lead to disciplinary action.

6.10. If you have any concerns about disclosing/sharing patient information you must discuss with your manager and if they are not available, someone with the same or similar responsibilities e.g. your Caldicott Guardian or Data Protection Officer/Head of Information Governance (see Appendix 3) If you cannot find anyone to discuss the issue with, you should take down the callers details and contact them when you are satisfied the disclosure of information can take place. The contact could be either via voice or electronic media.

6.11. **Telephone Enquiries**

6.12. If a request for information is made by telephone,

   • Always try to check the identity of the caller and check whether they are entitled to the information they request.

   • Take a number, verify it independently and call back if necessary.

6.13. Remember that even the fact that a patient is in hospital, a patient of the hospital or a member of staff, is confidential. If in doubt consult your manager or the Data Protection Officer. It is safer not to disclose than to disclose inappropriately.

6.14. **Requests for Information by the Police and media**

6.15. With respect to the Police

   • Requests for information from the Police should always be referred to the Data Protection Officer/Head of Information Governance or the
Records Services/PAS Manager. Access to these managers is available 24/7 via switchboard.

6.16. With respect to the Media

• Do not give out any information under any circumstances.

6.17. Only the Director of Communication/Press Officer are authorised to do so and are subject to national guidance on confidentiality in this respect. If you receive any request from the media by personal visit or by phone refer the person to the Trusts Press Officer.

RCHT
Press Office Number 01872 25 2934
Out of hours (24/7) Page via RCH switchboard

6.18. Remember, the media may not always make their status apparent. If you have any concerns about the validity of a caller or visitor, please contact the Press Office.

6.19. Disclosure of Information to Other Employees of the Trust

Information about patients should only be released on a need-to-know basis.

• Always check the member of staff is who they say they are.

• This can be achieved by checking the employee’s ID badge and/or their internal extension number or bleep number prior to giving them any information.

• If possible also check whether they are entitled to the information.

• Don’t be bullied into giving out information.

• If in doubt, check with the consultant/doctor in charge of the patient’s care. Or please contact either the Data Protection Officer or Records Services Manager.

6.20. Abuse of Privilege

6.21. It is strictly forbidden for employees to look at any information relating to themselves, their own family, friends or acquaintances unless they are directly involved in the patient’s clinical care or with the employees administration on behalf of the Trust. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

6.22. If you require to see your own Health Record, you should make a Subject Access Request to the Disclosure Office.
6.23. If you have concerns about this issue please discuss with your line manager.

6.24. **Carelessness**

- Do not talk about patients in public places or where you can be overheard. Please also be aware that talking about colleagues personal details, such as sickness or their financial details should also be avoided.

- Do not leave any Health Records or confidential information lying around unattended. Please ensure case notes are either locked in the appropriate trolley or face down to avoid casual observance.

- Make sure that the general public cannot see any computer screens, or other displays of information. This does not include the Whiteboards on wards as these have been given Information Governance clearance.

- When leaving your office, ensure you lock your PC, (Ctrl + Alt + Delete.)

- Secure all portable forms of data by locking them in a draw.

- Lock your office.

- You should not share your password with anyone, no matter how senior. (To do so would be a disciplinary offence)

- Do not transport confidential information in your car without adhering to the correct procedure. That being permission has been granted by a line manager, it is securely stowed in a secure bag in the boot of the vehicle you are in and not left unattended. If the records need to be kept overnight (again, with specific permission by a line manager) they should be placed securely in the home away from others who may visit or share the residence.

6.25. **Use of Internal and External Post**

6.26. Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

6.27. Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. ‘Confidential’ or ‘Addressee Only’, as appropriate. When received in the department only the Addressee may open the envelope unless others are authorised to do so.

6.28. External Mail must also observe these rules. Special care should be taken with personal information sent in quantity, such as case notes, or collections of patient records on paper, encrypted CD or other media. These should be sent by Special Delivery or by NHS courier. In some circumstances it is also
advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

6.29. Case notes and other bulky material should only be transported in the approved boxes/bags and never in dustbin sacks, carrier bags or other containers. Case notes for transit should not be left unattended unless stored, waiting for collection in a secure area.

6.30. If you are required to use your own vehicles to transport confidential information, it should be in an orange bag (where appropriate), in the boot of your car and not left unattended (unless as a part of an agreed working practice, normally where it would not be reasonable to take large quantities of records into a patient’s house). Records should not be left in vehicles overnight. They should be safely stored within the staff member’s premises.

6.31. Blood samples etc. and the accompanying request forms should be treated as confidential patient information and handled accordingly.

6.32. Faxing

6.33. All faxing of information should be carried out in line with the Trust Safehaven guidance which can be found within the Information Use Framework Policy in the Document Library on the Intranet/Internet.

6.34. Please see the Guidance for sharing personal information by Fax, which should be displayed in close proximity to the Fax Machine.

- Remove patient identifiable data from any faxes unless you are faxing to a known secure and private area (known as Safe Havens).
- Faxes should always be addressed to named recipients. Use a fax header sheet with your contact details.
- Always check the number to avoid misdialling and ring the recipient to check that they have received the fax.
- If your fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.

6.35. Storage of Confidential Information

6.36. Paper-based confidential information should always be kept locked away and preferably in a room that is locked when unattended, particularly at nights and weekends or when the building/office will be unoccupied for a long period of time.

6.37. PC-based information should not be saved onto local hard drives or onto removable media, but onto the Trust network, CDs, and other media should be kept in locked storage.

6.38. Encrypted memory sticks can be provided in some exceptional circumstances with the authorisation of line managers. Please contact CITS for advice.
6.39. **Disposal of Confidential Information**

6.40. When disposing of paper-based person-identifiable information or confidential information always use ‘Confidential Waste’ sacks/shredders. Keep the waste in a secure place until it can be collected for secure disposal.

6.41. Computer printouts should either be shredded or disposed of as paper-based confidential waste.

6.42. CDs containing confidential information must be destroyed once they have fulfilled their use. Computer files with confidential information no longer required must be deleted from the server if necessary (no data is to be stored on the hard drives of PC’s). Destroy CDs by cutting through the disc.

6.43. Computer hard disks are only to be destroyed/disposed of by the IT experts within the Trust. Please contact Cornwall IT Services for them to collect the drives for destruction. This is to ensure all information is deleted from the disk, as even by re-formatting it is possible to gain access to the original data.

6.44. Patient Identifiable Information must be kept for a set period of time. This is outlined within Clinical Records Retention Schedule. This indicates the minimum time for which both medical and business NHS records should be retained and sets out the legal obligations for all NHS bodies to keep proper records and the rules on archiving or destruction. The Trust has a Records Management Strategy which has been endorsed by the Trust Board.

6.45. Further information is available from the Document Library.

6.46. **Confidentiality of Passwords, PIN numbers, etc**

6.47. Personal passwords, PIN numbers, etc issued to or created by employees should be regarded as confidential and they must not be communicated to anyone.

Passwords, PIN numbers, etc should not be written down.

Passwords, PIN numbers, etc should not relate to the employee or the system being accessed.

6.48. You will be given more information about their control and format etc. when you receive your training and/or password, PIN, etc.

6.49. No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords, PINs, etc or privileges issued to other employees. Any attempts to breach security should be immediately reported to the IT Security Manager and may result in disciplinary action. It may be considered as a breach of the Computer Misuse Act 1990 and/or the Data Protection Act and may result in a disciplinary action and/or legal proceedings.
6.50. **Emailing Confidential Information**

6.51. Please see the “Email Policy” available on the Document Library.

6.52. Patient identifiers should be removed wherever possible, and only the minimum necessary information sent. Names, dates of birth or other strong identifiers should not be used in the subject heading. A CR number maybe used as it is a pseudonym.

6.53. Special care should be taken to ensure the information is sent only to recipients who have a “need to know”; always double check you are sending the mail to the correct person/s.

6.54. Please ensure you check the nhs.net account details of those working in other Trusts, this can be done via the Telephone Directory link on the home page of the Intranet. The link is https://web.nhs.net/public/?a=s

6.55. External transfers should only take place to persons with access to nhs.net/N3 or approved recipients. Under no circumstances whatsoever should any type of patient identifiable information or sensitive or confidential information about any other person be e-mailed to persons who only have a Hotmail account, without the permission of your line manager or the Data Protection Officer. Due to its unsecure nature, any information transmitted over the Internet should be considered to be in the public domain.

6.56. See the Trust E-mail policy for more detailed information.

6.57. **Working at home**

6.58. The Organisation does not advocate the taking of person identifiable Information or Records home for any reason. If you feel you have reason to do so, you MUST contact the Records Services Manager if they are clinical records or the Corporate Records Manager if they are corporate or business records to discuss prior to taking any records off site.

6.59. If you do have a justifiable reason to take patient or corporate records home, you must ensure they are securely stored to prevent accidental or malicious access by non authorised people. It will be your responsibility to ensure they are recorded as being in your possession and that they are safely returned.

6.60. **Copying of software**

6.61. All computer software used with the Trust is regulated by license agreements. A breach of the agreement could lead to legal action against the organisation and/or the offender (member of staff).

6.62. It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use. This would be a breach of the license agreement.
6.63. **General provisions**

6.64. **Interpretation**

6.65. If any person requires an explanation concerning the interpretation or the relevance of this code of conduct, they should discuss the matter with their line manager, Head of Information Governance/ Trust Data Protection Officer, Caldicott Guardian or the Records Services and PAS Manager.

6.66. **Non-Compliance**

6.67. Non-compliance with this code of conduct by any person working for the Trust may result in disciplinary action or criminal charges being taken in accordance with the Trust disciplinary procedure, and may lead to dismissal for gross misconduct.

6.68. Breaches of the Data Protection Act 1998 could result in a fine for the Trust from the Information Commissioners Office which could amount to £500,000.

6.69. Anyone found breaching confidentiality could be sued by the data subject up to £5000.

6.70. A record is kept of everyone who accesses information held on the Trusts patient based systems which is audited and can be made available to the patient.

6.71. To obtain a copy of the disciplinary procedures please look on the Document Library or discuss with your line manager.

7. **Dissemination and Implementation**

7.1. This document will be submitted to the Information Governance Committee for approval and following approval will be disseminated to staff via the management structure. New and existing staff will be notified via the ‘All Users Bulletin when the policy is made available on the Document Library: They will be made aware of its contents during relevant Information Governance training in line with the Training Needs Analysis as outlined in the RCHT Core Training Policy.

8. **Monitoring compliance and effectiveness**

<table>
<thead>
<tr>
<th>Element to be monitored</th>
<th>This Policy will be monitored entirety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead</td>
<td>Although the Head of Information Governance will lead this, it the responsibility of all line managers to monitor their own areas of influence.</td>
</tr>
<tr>
<td>Tool</td>
<td>Datix will be used to monitor the incidents and risks that are relevant to the content of the Code of Conduct.</td>
</tr>
<tr>
<td>Frequency</td>
<td>The management of risks and incidents is an ongoing process resulting in real time continuous monitoring.</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Reporting arrangements | The Information Governance Committee will receive reports at each meeting; these will be tabled by the Head of Information Governance.  
The IGC meets bi-monthly. |
| Acting on recommendations and Lead(s) | Any recommendations or actions will be delegated to the relevant departmental lead as required.  
A report on progress will be required as directed by the agreed timescale for completion. |
| Change in practice and lessons to be shared | Significant changes to working practices will be disseminated via the All Users Bulletins  
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. The Code of Conduct for Employees in Respect of Confidentiality is updated and reviewed annually

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. **Equality Impact Assessment**

10.3. The Initial Equality Impact Assessment Screening Form is at Appendix 2.
### Appendix 1. Governance Information

<table>
<thead>
<tr>
<th>Document Title</th>
<th>The Code of Conduct for Employees in Respect of Confidentiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Issued/Approved:</td>
<td>22 September 2014</td>
</tr>
<tr>
<td>Date Valid From:</td>
<td>22 September 2014</td>
</tr>
<tr>
<td>Date Valid To:</td>
<td>22 September 2017</td>
</tr>
<tr>
<td>Directorate / Department responsible (author/owner):</td>
<td>Mark Scallan</td>
</tr>
<tr>
<td>Contact details:</td>
<td>01872 258580</td>
</tr>
<tr>
<td>Brief summary of contents</td>
<td>A code of conduct to inform staff how to handle person identifiable information securely.</td>
</tr>
<tr>
<td>Suggested Keywords:</td>
<td>Code of Conduct, Confidentiality, Data Protection, Information sharing, Information Governance</td>
</tr>
<tr>
<td>Target Audience</td>
<td>RCHT</td>
</tr>
<tr>
<td>Executive Director responsible for Policy:</td>
<td>Director of Finance</td>
</tr>
<tr>
<td>Date revised:</td>
<td></td>
</tr>
<tr>
<td>This document replaces (exact title of previous version):</td>
<td>Code of Conduct for Employees in Respect of Confidentiality</td>
</tr>
<tr>
<td>Approval route (names of committees)/consultation:</td>
<td>Information Governance Committee</td>
</tr>
<tr>
<td>Divisional Manager confirming approval processes</td>
<td>Head of Quality, Safety and Compliance</td>
</tr>
<tr>
<td>Name and Post Title of additional signatories</td>
<td>Not Required</td>
</tr>
<tr>
<td>Signature of Executive Director giving approval</td>
<td>{Original Copy Signed}</td>
</tr>
<tr>
<td>Publication Location (refer to Policy on Policies – Approvals and Ratification):</td>
<td>Internet &amp; Intranet</td>
</tr>
<tr>
<td>Document Library Folder/Sub Folder</td>
<td>Health Informatics /Information Governance</td>
</tr>
<tr>
<td>Links to key external standards</td>
<td>Information Governance Toolkit</td>
</tr>
</tbody>
</table>
Version Control Table

<table>
<thead>
<tr>
<th>Date</th>
<th>Version No</th>
<th>Summary of Changes</th>
<th>Changes Made by (Name and Job Title)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V1.5</td>
<td>Initial Issue</td>
<td>Mark Scallan Head of Information Governance</td>
</tr>
<tr>
<td>19 Nov 12</td>
<td>V2.0</td>
<td>Updated to reflect compliance needs with the Policy on Policies. Previous version</td>
<td>Mark Scallan Head of Information Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>history not known</td>
<td></td>
</tr>
<tr>
<td>3 Sep 14</td>
<td>V2.5</td>
<td>Updated to reflect compliance needs with the Policy on Policies. Also changes made</td>
<td>Mark Scallan Head of Information Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to reflect organisational changes and the use of nhs.net by partner organisations.</td>
<td></td>
</tr>
</tbody>
</table>

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 2. Initial Equality Impact Assessment Form

Name of the strategy / policy / proposal / service function to be assessed (hereafter referred to as policy) (Provide brief description):

<table>
<thead>
<tr>
<th>Directorate and service area: Information Governance</th>
<th>Is this a new existing Policy.</th>
</tr>
</thead>
</table>

Name of individual completing assessment: Mark Scallan

<table>
<thead>
<tr>
<th>Telephone: 01872 258580</th>
</tr>
</thead>
</table>

1. Policy Aim*
Who is the strategy / policy / proposal / service function aimed at?

To inform staff of their responsibilities with regards to confidentiality.

2. Policy Objectives*
To ensure person identifiable data is handled securely through staff awareness.

3. Policy – intended Outcomes*
To minimise incidents and risks associated with the handling of confidential information.

4. *How will you measure the outcome?
Through Datix reports and spot checks.

5. Who is intended to benefit from the policy?
All staff who handle person identifiable information.

6a) Is consultation required with the workforce, equality groups, local interest groups etc. around this policy?
No

b) If yes, have these *groups been consulted?

C). Please list any groups who have been consulted about this procedure.

7. The Impact
Please complete the following table.

Are there concerns that the policy could have differential impact on:

<table>
<thead>
<tr>
<th>Equality Strands:</th>
<th>Yes</th>
<th>No</th>
<th>Rationale for Assessment / Existing Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td></td>
<td></td>
<td>No equality issues.</td>
</tr>
<tr>
<td>Sex (male, female, transgender / gender reassignment)</td>
<td></td>
<td></td>
<td>No equality issues.</td>
</tr>
<tr>
<td>Race / Ethnic communities /groups</td>
<td>No equality issues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disability -</td>
<td>No equality issues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learning disability, physical disability, sensory impairment and mental health problems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religion / other beliefs</td>
<td>No equality issues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marriage and civil partnership</td>
<td>No equality issues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pregnancy and maternity</td>
<td>No equality issues.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual Orientation, Bisexual, Gay, heterosexual, Lesbian</td>
<td>No equality issues.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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

Names and signatures of members carrying out the Screening Assessment  
1.  
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 ____________________________
Appendix 3. Contact Information

Caldicott Guardian

Royal Cornwall Hospital NHS Trust

Dr Rob Parry
Caldicott Guardian
Head Office
Bedruthan House
Penventinnie Lane
Truro
TR1 3LJ

Tel: 01872 25 2223
Fax: 01872 25 2944

Data Protection Officer

Royal Cornwall Hospital NHS Trust

Mr Mark Scallan
Head Information Governance
2nd Floor Knowledge Spa
Royal Cornwall Hospital
Truro TR1 3LJ

Tel: 01872 25 8580