CONFIDENTIALITY POLICY

1. INTRODUCTION

1.1 Confidentiality is fundamental to patient care and the employment of staff. Any breach of confidentiality to an unauthorised person, however innocently made, will be treated seriously, in line with the Trust's disciplinary procedures.

1.2 An authorised person is an individual or organisation designated by statute, by NHS or trust policy to have access to personal information (either patient data or other categories of personal data), as necessary in the course of their duties. It is important to note that any information that an authorised person receives during the course of their duties must only be used for authorised purposes (e.g. to support the clinical care of a patient, either directly or indirectly) – any other use is strictly forbidden.

1.3 This policy is aligned with the Trust's Proud to Care values (Compassion, Achievement, Relationships, Environment) Further information on the Trust's values is available on the intranet.

1.4 This policy should be read alongside the Trust's Acceptable Use policy to ensure there is an awareness of all IG requirements.

2. POLICY STATEMENT

2.1 The principles set out in this policy apply to all those working in the Trust, including: employees; staff employed by outside agencies but working on the premises; those employed on unpaid honorary contracts; Non-Executive Directors, volunteers, or those based in the Trust for the purpose of training.

2.2 There is national legislation/guidance and Trust policies related to this policy that Trust employees will need to be aware of and consult where relevant, details of these can be found in sections 16 and 17.

2.3 As a result of the diverse nature of services provided at the Trust directorates may have supplementary and complementary local policies and procedures. Anyone with access to Trust information has a responsibility to establish if such policies and procedures are in place. Local directorate policies will be explained to new starters during local induction, and updates will be circulated thereafter as appropriate.

2.4 Increasingly, confidential personal information is held on computers. The Trust has an established Caldicott Guardian role, held by the Medical Director, and a Senior Information Risk Officer, held by the Director of Nursing & Patient Care, to oversee the management of all Information Governance issues and implement appropriate governance arrangements, policy and procedures. Every IT system holding personal data is required by Trust policy to have arrangements for securing this data (see the IM&T Security Policy Organisational Policy 2.17).

3. EQUALITY IMPACT ASSESSMENT

3.1 The Trust aims to design and implement services, policies and measures that meet the diverse needs of services, the population and workforce, ensuring that none are placed at a disadvantage over others.

3.2 Therefore, this policy and procedure applies to all Trust employees irrespective of age, race, colour, religion, belief, disability, nationality, ethnic origin, sexual orientation or marital status, carer status, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership. All employees will be treated in a fair and equitable manner.

3.3 The Trust will take account of any specific access or specialist requirements for individual employees during the implementation of this policy.

4. PATIENT INFORMATION

4.1 All patients have the right to expect complete confidentiality in relation to their care and treatment. It is breach of confidentiality to:

4.1.1 Disclose to an unauthorised person the fact that a patient has been identified as being on the premises.

4.1.2 Disclose to an unauthorised person any detail about a patient's condition, treatment, or any other detail about a patient gained in the course of working within the Trust.

4.1.3 Young people aged 16 years and over are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidentiality as adults. Children under the age of 16 who have the capacity to make decisions about their own treatment are also entitled to make decisions about the use and disclosure of information they have provided in confidence. Information held must not be shared with others including those with parental responsibility without the consent of the young person, if they are competent to give it (see Consent to Examination or Treatment Policy, Clinical Practices Policy 2.40).

4.1.4 Use information gained about patients in the course of working within the Trust for purposes other than those genuinely connected with the care and treatment of the Trust's patients. See the Research Policy Organisational Policy 1.17 for confidentiality issues in relation to research.

4.2 All those working within the Trust must therefore ensure that they do not:

4.2.1 Divulge confidential information concerning patients to unauthorised persons.

4.2.2 Discuss confidential information concerning patients in a way which might lead to accidental disclosure in public areas, such as corridors, lifts, dining areas or recreational areas within the Trust's premises and includes the use of other electronic communication methods including social networking sites.

4.2.3 Discuss confidential information concerning patients outside the Trust's premises in a way, which might lead to unauthorised persons gaining such information.

4.2.4 Use information gained about patients in the course of working within the Trust for their own purposes.

4.3 All those working within the Trust must equally ensure that they always:

4.3.1 Refer enquiries from the media to the Head of Communications in the first instance, or to a Senior Manager in the Division. Outside normal working hours, press enquiries should

be reported to the Head of Communications or the Site Matron/Night Matron (see Communications (Media Handling) Policy Organisational Policy 4.13).

4.3.2 Refer enquiries about patients from the police, solicitors or other agencies and organisations to their manager in the first instance, or in their absence the Senior Manager in the Division, or outside normal working hours, to the Site Matron/Night Matron.

4.3.3 Refer to their line manager for advice in situations in which a breach of confidentiality may have potentially occurred, either by themselves or by others.

4.3.4 Recognise the confidential and sensitive nature of patient's health care records including (but not limited to) clinical records and other patient related information. Handover sheets should be shredded once no longer needed. Health care records must be stored and handled with care and discretion (see Health Care Record Management Policy, Organisational Policy 4.18). Healthcare records must not be taken off Trust premises, except where specifically authorised. Where patients are reviewed in the community using records other than hand-held, the record must be returned to Trust premises as soon as possible and must not be kept by the health professional overnight.

5. FORMAL CORRESPONDENCE WITH PATIENTS AND OTHER HOSPITALS

5.1 Correspondence with patients detailing appointments and any other information must be sent in unmarked envelopes and not franked with the Trust's logo.

5.2 Clinical information must be marked "confidential". Correspondence must always be securely parcelled. Confidential correspondence must never be sent by unsecured taxi, but only via a Trust approved courier service.

6. RECEIPT OF ENQUIRIES ABOUT PATIENTS

6.1 When requests are received seeking information about patients in the Trust, such information must not be disclosed without the prior permission of the patient. Local arrangements will have to be developed to ensure those with legitimate concerns have access to information.

6.2 Where, in the judgement of an Executive Director of the Trust, and, if necessary, taking legal guidance into account, the failure to release the information would be contrary to the public interest, the NHS, or the interest of the patient concerned, information may be released.

6.3 Where telephone or face-to-face enquiries are seeking information about patients, the person receiving the enquiry must establish the identity of the enquirer before patient details are given.

6.4 If the caller is from another hospital or GP and is seeking information which may affect the care of the patient, the identity of the enquirer must be confirmed and if there is any uncertainty, a return call must be made to confirm the caller's identity. If there remains any doubt this should be referred to the Divisional General Manager or equivalent.

6.5 Media enquiries requesting information about patients in the Trust must be referred to the Head of Communications or a Senior Manager in the Division (see Communications (Media Handling) Policy Organisational Policy 4.13).

6.6 Further information, clarification or advice about patient confidentiality can be sought from the Director of Nursing & Patient Care. Further information on Information Governance issues should also be referred to the Caldicott Guardian (Medical Director).

7. RECEIPT OF ENQUIRIES REGARDING OR RELATING TO EMPLOYEES

7.1 All employees of the Trust have the right to expect that details of their employment with the Trust will be held in confidence. This principle extends to and includes the use of other electronic communication methods including social networking sites. It will therefore be a breach of confidentiality to:

7.1.1 Disclose to an unauthorised person the fact that a person is employed by the Trust.

7.1.2 Disclose to an unauthorised person any detail relating to the person's employment, or any other information about an employee gained in the course of working within the Trust.

7.1.3 Use information gained about an employee in the course of working within the Trust for purposes other than those genuinely connected with the Trust's business.

7.2 Information will only be disclosed with the express permission of the employee, except where in the judgement of an Executive Director it would be prejudicial to the public interest, the Trust or the employee concerned not to release the information.

7.3 All those working within the Trust must ensure that they do not:

7.3.1 Divulge confidential information concerning employees to unauthorised persons. It is accepted that in certain situations, in particular where telephone calls are received asking for employees by name, it may be impossible to avoid disclosing the fact that a person works within the Trust. In these situations, staff receiving calls should refer to their manager for advice.

7.3.2 Discuss confidential information concerning employees in a way that might lead to accidental disclosure in public areas within the Trust's premises.

7.3.3 Discuss confidential information concerning employees outside the Trust's premises in a way that might lead to unauthorised persons gaining such information.

7.3.4 Use information gained about other employees in the course of working within the Trust for their own purposes.

7.4 Trust employees should ensure that they always:

7.4.1 Refer enquiries about staff from the media, police, solicitors, Department of Social Security or other organisations/agencies to their Manager.

7.4.2 Refer to their manager for advice in situations in which a breach of confidentiality may potentially have occurred either in relation to things that they have done or those that they know other people have done.

7.5 Further information, clarification or advice about employee confidentiality can be obtained from the Corporate Secretary.

8. FORMAL CORRESPONDENCE WITH EMPLOYEES

8.1 Any correspondence addressed to an employee of Chesterfield Royal Hospital NHS Foundation Trust which is of a personal nature must be marked "Personal and in Confidence".

8.2 It is the responsibility of individual members of staff to ensure that any change of address is notified on an amendment form.

9. REQUEST FOR FINANCIAL REFERENCES

9.1 Requests for financial references such as those from a bank and/or building society, are processed by Pay Services and will need to be supported by written authority for disclosure from the employee. If such authority is not available, it must be obtained before any disclosure is made.

10. COMPUTERISED INFORMATION

10.1 The safe management of computerised personal data is a priority for the Trust (see the IM&T Security Policy Organisational Policy 2.17). Loss or accidental disclosure of data held on CDs or memory sticks, or on paper print outs or in any other format whatsoever will be treated as a potential Serious Incident (SI). Users must ensure that that they handle all removable media in accordance with trust policy. If in doubt, guidance should be sought from the Information Governance Officer.

10.2 Similarly, electronic transmission of personal data by email or other mechanism must always be encrypted, and/or follow procedures as defined in the Caldicott Guardian's approval of the data flow. No personal data should be transmitted without this approval.

10.3 Personal passwords have been introduced to protect the integrity of IT systems containing personal information. IT system users must ensure the protection of their passwords at all times

11. USE OF FACSIMILE (FAX) MACHINES – THE SAFE HAVEN POLICY

11.1 The Trust has established a policy to regulate the use of fax machines to transmit personal data (see the Information 'Safe Haven' Policy Organisational Policy 4.35). In summary, all transmissions of personal data by fax may only be made from specially designated fax machines, and must be properly recorded and checked against the possibility of accidental re-direction. There are no exceptions to this policy. Users must check the local 'Safe Haven' procedure before using any fax machine.

12. COMMERCIAL IN CONFIDENCE ISSUES

12.1 Information about the operation of the Trust and its financial arrangements may be considered commercially sensitive. The Trust also receives information from other organisations which we are obliged to ensure remains confidential.

12.2 Employees should be particularly careful of using, or making public, internal information of "Commercial in Confidence" nature, particularly if its disclosure would prejudice the principle of fair competition. This principle applies whether private competitors or other public sector providers are concerned, and whether or not disclosure is prompted by the expectation of personal gain (see the Standing Financial Instructions).

13. RELATIONSHIPS WITH THE MEDIA

13.1 As a representative of the Trust employees should refer media enquiries regarding patients, staff and the Trust's business to the Head of Communications. Requests for patient condition checks can be answered by the staff members, see section 2.4 of the Communications (Media Handling) Policy Organisational Policy 4.13.

13.2 Staff may approach the media using the guidelines outlined in the Voicing Your Concerns policy (Personnel Policy No. 33). Any breach of confidentiality made by releasing information to the media is regarded as an extremely serious issue. Further guidance on the Trust's and staff relationship with the media is available from the Head of Communications.

13.3 Any issues relating to government, statutory or Trust policy must be directed to an Executive Director or in their absence the Site/Night Matron must be contacted.

14. STAFF CONCERNS

14.1 Employees wishing to raise concerns regarding patient care, or the activities of the Trust, should follow the Voicing Your Concerns policy (Personnel Policy No. 33). An individual summary of the policy has been distributed to all staff and is issued to all new starters. Every reasonable action must be taken to resolve issues locally and informally.

15. TRAINING REQUIREMENTS

15.1 The requirement to maintain confidentiality is included in all employees contract of employment.

15.2 Managers must ensure that this Trust-wide policy along with directorate and local arrangements on confidentiality are brought to the attention of all those in their directorate as identified in 1.5.

15.3 Following ratification of this policy it will be confirmed in Core Brief and the pay slip bulletin.

16. MONITORING

16.1 Adherence to the policy is monitored by incident reporting and the review of those incidents by the directorate governance group(s) and appropriate Trust committee(s).

17. KEYWORDS

17.1 Whistle blowing, whistleblowing,

18. REFERENCES

18.1 Access to Health Records Act 1990
Data Protection Act 1998;
The Human Rights Act 1998
Freedom of Information Act 2000
Confidentiality NHS Code of Practice DH 2003
Records management: NHS Code of Practice DH 2006
Healthcare professional organisations' Codes of Conduct
Information Governance Serious Untoward Incident Guidance

19. RELATED POLICIES

19.1 Access to Healthcare Records Organisational Policy 1.6
Acceptable Use policy
Communications (Media Handling) Policy, Organisational Policy 4.13
Consent to Examination or Treatment Policy, Clinical Practices Policy 2.40
Disciplinary Procedure Personnel Policy No. 3
E-Mail Policy, Organisational Policy 4.22
IM&T Security Policy, Organisational Policy 2.17
Healthcare Record Keeping Policy, Organisational Policy 4.12
Health Care Record Management Policy, Organisational Policy 4.18
Information 'Safe Haven' Policy, Organisational Policy 4.35
Making and Using Visual and Audio Recordings of Patients Organisational Policies 1.31
Police Access to Personal Health Information, Organisational Policy 1.9
Policy for Access to Legal Services, Organisational Policy 4.21
Policy for Remote Access to Trust IT Systems, Organisational Policy 4.34
Policy for the Use and Secure Disposal of Removable Storage Media, Organisational Policy 4.44
Research Policy, Organisational Policy 1.17

Standing Financial Instructions
Use of Mobile Phones And Hand Held Transceivers, Organisational Policy 4.16
Voicing Your Concerns Policy, Personnel Policy No. 33

Date ratified:	Staff Partnership Committee – March 2017
First issued:	May 1995
Version no.:	2.0
Date issued:	March 2017
Review date:	March 2019
For review by:	Head of Human Resources/Head of Health Informatics
Director responsible:	Director of Nursing & Patient Care

EQUALITY IMPACT ASSESSMENT APPENDIX 1

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

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**	No	
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability – learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?**		
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**Is so can the impact be avoided?**		
6.	**What alternative are there to achieving the policy/guidance without impact?**		
7.	**Can we reduce the impact by taking different action?**		