Data Protection and Information Sharing:
Information Governance ("IG") Policy
(in incorporating the Confidentiality Code of Conduct, Information Sharing Policy, Safe Haven and Pseudonymisation procedures)

FINAL 3.2, Jan 2018
SUMMARY

This Policy:

- Ensures that all managers and staff are aware of and comply with the Trust’s statutory obligations and responsibilities, including those under the Data Protection Act (DPA), and the new General Data Protection Regulations (GDPR).
- Provides guidance on the rights of individuals under the Common Law Duty of Confidentiality and other legislation as appropriate, and outlines the arrangements adopted by the Trust for the auditing and monitoring of confidentiality and data protection within the organisation.
- Provides clear and robust information sharing, safe haven, anonymisation and pseudonymisation procedures across the Trust, with guidance on the use of patient information for clinical training, research and systems testing.

DOCUMENT DETAILS

<table>
<thead>
<tr>
<th>Author(s):</th>
<th>Information Governance Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td>January 2018 [FINAL 3.2]</td>
</tr>
<tr>
<td>Next Review Date:</td>
<td>January 2021 (3-yearly)</td>
</tr>
<tr>
<td>Ratifying Body/Committee:</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>Chair:</td>
<td>Senior Information Risk Owner (SIRO)</td>
</tr>
<tr>
<td>Date Originally Ratified:</td>
<td>29 August 2014</td>
</tr>
<tr>
<td>Target Audience:</td>
<td>All Staff</td>
</tr>
<tr>
<td>Date Equality Impact Assessment Completed:</td>
<td>April 2014 / November 2017</td>
</tr>
</tbody>
</table>

DOCUMENT HISTORY

<table>
<thead>
<tr>
<th>Date of Issue</th>
<th>Version No.</th>
<th>Next Review Date</th>
<th>Date Approved</th>
<th>Director Responsible for Change</th>
<th>Nature of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2018</td>
<td>Final 3.2</td>
<td>Jan 2021</td>
<td>08 Jan 2018</td>
<td>SIRO/Caldicott Guardian</td>
<td>Implications of the GDPR. Merged with Information Sharing Policy.</td>
</tr>
<tr>
<td>Apr 2015</td>
<td>Final 2.0</td>
<td>Aug 2017</td>
<td>29 May 2015</td>
<td>SIRO/Caldicott Guardian</td>
<td>Addition of TNA and change to audit process</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1. RELEVANT TO ........................................................................................................... 3
2. PURPOSE ...................................................................................................................... 4
3. GENERAL PRINCIPLES ............................................................................................. 5
   - Legislations, Regulations and Guidance ................................................................. 5
   - Data Protection ....................................................................................................... 6
   - Information Sharing ............................................................................................... 6
   - Staff Responsibilities ............................................................................................. 7
4. DIFFERENT INFORMATION TYPES .......................................................................... 8
   - 4.1. Personal Information ....................................................................................... 8
   - 4.2. Special Categories of Personal Information ...................................................... 8
   - 4.3. Confidential Information ............................................................................... 9
   - 4.4. Audio Recordings, Photographs and Other Images .......................................... 9
   - 4.5. Closed Circuit Television (CCTV) .................................................................. 9
5. DATA PROTECTION .................................................................................................... 10
   - 5.1. Data Protection Principles .......................................................................... 10
   - 5.2. General Computer/Systems Security .............................................................. 11
   - 5.3. General Security Measures ........................................................................ 12
6. THE CALDICOTT PRINCIPLES ................................................................................ 13
7. CONFIDENTIALITY ..................................................................................................... 14
8. CONSENT TO THE COLLECTION, USE AND SHARING OF INFORMATION .......... 14
   - 8.1. General Conditions for Consent .................................................................. 14
   - 8.2. Patient Information ...................................................................................... 15
   - 8.3. Information about Children and Young People .............................................. 16
   - 8.4. Information about Individuals Lacking Capacity ............................................ 16
   - 8.5. Staff Information ......................................................................................... 16
9. IMAGES, AUDIO AND VIDEO – CLINICAL AND NON-CLINICAL USE ................. 17
   - 9.1. Definitions and General Principles ............................................................... 17
   - 9.2. Clinical Purposes ......................................................................................... 18
   - 9.3. Clinical Images for Non-Clinical Purposes .................................................. 18
   - 9.4. Media and Other Promotional Use ............................................................... 18
   - 9.5. Personal Photos ........................................................................................... 19
10. INFORMATION SHARING .......................................................................................... 20
    - 10.1. Principles of Information Sharing .............................................................. 20
    - 10.2. Information Sharing for Care Purposes ...................................................... 21
    - 10.3. Information Sharing Agreements/Protocols/Contracts .............................. 21
    - 10.4. Disclosure of Information to the Police ...................................................... 22
    - 10.5. Transfers Outside of the European Economic Area (EEA) .................... 23
    - 10.6. Freedom of Information (FOI) Requests ................................................... 23

---

Author: Information Governance Officer  
Policy Date: January 2018  
Review Date: January 2021
The purpose of this policy is to ensure that there is a consistent, fair and transparent approach in its application across Poole Hospital NHS Foundation Trust (hereafter referred to as the “Trust” or the “organisation”). All managers and staff (at all levels) are responsible for ensuring that they are viewing and working to the current version of this policy. If this document is printed in hard copy or saved to another location, it must be checked that the version number in use matches with that of the live policy on the intranet. All policy are published on the staff intranet and communication is circulated to all staff when new policies or changes to existing policies are released. Managers are encouraged to use team briefings to aid staff awareness of new and updated policies.
THE POLICY

1. RELEVANT TO

1.1. All medical and non-medical individuals at all levels within Poole Hospital NHS Foundation Trust (“the Trust”) are expected to comply with this policy, including: individuals directly employed by the Trust (substantive/permanent, fixed-term, bank/locum, etc); and individuals working within but not directly employed by the Trust (volunteers, students, agency, secondees, etc); hereafter referred to collectively as “staff”.

1.2. This policy covers all aspects of information within the Trust and is not solely patient/service user related. Information produced, handled and held by the Trust includes, but is not limited to:

- patient/client/service user information;
- staff/personnel information;
- corporate/business Information.

Further details and definitions can be found in Section 4 of this policy.

1.3. This policy covers all methods of holding information and in all media, including, but not limited to:

- systems purchased/developed/managed by, or on behalf of, the Trust;
- manually stored data in paper format;
- tapes and other data from CCTV systems;
- data held in offsite archive storage;
- data held on CDs/DVDs, memory sticks, laptops, ipads, iphones, and all other types of mobile media;
- structured and unstructured record systems – paper and electronic;
- transmission of information – email, post, fax and telephone.

1.4. This policy should be read in conjunction with other relevant policies, procedures and guidance, including the:

- Informatics (IT) Policies and Procedures
- Medical Records Policy and Procedures
- Policy for Obtaining Consent for Treatment from Adults and Children
- Data Security Statement (Information Governance Confidentiality & IT)
- Subject Access and Other Information Rights Policy
- Privacy Notices (Patient/Service User and Staff Information)
- ICO Privacy Notices, Transparency and Control Code of Practice
- IGA Records Management Code of Practice
- NHS Digital Code of Practice on Confidential Information
- NHS Confidentiality Code of Practice
- CQC Code of Practice on Confidential Personal Information
- HSCIC Guide to Confidentiality in Health and Social Care
2. PURPOSE

2.1. This policy ensures that all managers and staff are aware of and comply with the Trust’s statutory obligations and responsibilities, including those under the Data Protection Act (DPA), and the new General Data Protection Regulations (GDPR) which takes effect from May 2018.

2.2. This policy provides guidance on the rights of individuals under the Common Law Duty of Confidentiality and other legislation as appropriate, and outlines the arrangements adopted by the Trust for the auditing and monitoring of confidentiality and data protection within the organisation.

2.3. This policy aims to provide clear and robust information sharing procedures to ensure that the Trust is designated as a ‘Safe Haven’ and meets national standards regarding the receipt and transfer of information. This policy includes guidance on the use of patient information for clinical training, research and systems testing and provides an understanding and procedure for the different means of communicating personal and confidential information.

2.4. This policy ensures that external partner organisations are fully confident that any personal and confidential information released to the Trust will be protected and processed in accordance with the associated information sharing agreements, as well as the commitments of the:

   a. Dorset Care Record;
   b. Dorset Information Sharing Protocol (DISC);
   c. Multi-Agency Risk Assessment Conferences (MARACs) Information Sharing Protocol for Bournemouth, Dorset and Poole;
   d. Personal Information Sharing Agreement (PISA) with the Bournemouth and Poole Safeguarding Adults Board;
   e. Children and Young People Partnerships Multi-Agency Data and Information Sharing Protocol for Bournemouth, Dorset and Poole;

   and any other local, regional or national information sharing initiatives to which the Trust is an approved signatory.

2.5. The Trust, and individual members of staff, have a legal obligation to comply with all appropriate legislation in respect of information handling, information security and confidentiality. This policy does not allege to cover all situations; therefore the responsibility lies with staff/departments to ensure that the confidentiality/security of information is maintained whilst under their ownership and to seek advice from senior management or the Information Governance Department as necessary.
3. GENERAL PRINCIPLES

Legislations, Regulations and Guidance

3.1 The Trust’s Data Protection Officer is the Information Governance Manager. The Trust has an obligation as a Data Controller to notify the Information Commissioner’s Office (ICO) of the purposes for which it processes personal data. The Trust’s ICO Registration Number is Z5566239:

https://ico.org.uk/ESDWebPages/Entry/Z5566239

3.2 The Data Protection Act (DPA) is the main piece of UK legislation which governs the use of personal data which identifiable living individuals. The General Data Protection Regulation (GDPR) takes effect from 25 May 2018 and will replace the 1995 data protection directive which originated the DPA. This policy has been revised to reflect the Trust’s obligations under the new EU GDPR and the updated DPA in the UK.

3.3 The GDPR is intended to strengthen and unify data protection for individuals within the EU, and address the security of transferring personal data outside the EU. It therefore applies to all information processing carried out by organisations operating within the EU, and organisations outside the EU that offer goods or services to individuals in the EU. The UK’s decision to leave the EU will not affect the expectation for UK organisations to be compliant with the GDPR from May 2018.

3.4 There are other rules and regulations which specify how information should be handled. These include, but are not limited to:

- Access to Health Records 1990
- Access to Medical Reports Act 1998
- Code of Practice on Confidential Information 2014
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Confidentiality NHS Code of Practice
- Crime and Disorder Act 1998
- Criminal Justice and Immigration Act 2008
- Freedom of Information Act 2000
- HMG: Information Sharing by Practitioners in Safeguarding Services
- HSCIC Guide to Confidentiality 2013
- Human Rights Act 1998 (Article 8)
- Information Security NHS Code of Practice
- NHS Care Record Guarantee for England
- Mental Capacity Act 2005
- Records Management Code of Practice 2016
- Social Care Record Guarantee for England
Data Protection

3.5 Personal and confidential information must only be used for the purpose(s) for which it was obtained. For example, information held on a patient or staff administration system must not be used to look up the addresses or birthdays of family, friends or colleagues.

3.6 Staff should only collect and keep the minimum amount of information that they require for the intended purpose. It is not acceptable to hold information unless there is a clear view as to how it will be used. It is not acceptable to hold information ‘just in case it might be useful later’.

3.7 Unless there is a legally acceptable condition for processing or sharing the information, explicit consent must be obtained from the data subject. This must be provided in writing and without coercion – it is not acceptable to assume an individual’s consent or rely on implied (unstated) consent unless a legal exemption applies (see 5.1.2(1) and Appendix B).

3.8 All data breaches, incidents and near-misses must be reported via the adverse incident reporting process (Datix). Where it involves the inappropriate destruction or alteration, loss/theft or unauthorised disclosure (or access to) personal or confidential information, the Information Governance Department must be informed immediately to assess the severity of the breach and support with identifying the remedial action required. Every incident must be reviewed by the Information Governance Department to establish if it is reportable to the ICO, which must happen within 72 hours of identification. Failing to notify the ICO of a breach when required to do so, or unnecessarily delaying notification, can result in significant financial consequences. Further guidance is available within the Information Risk and Security Policy.

Information Sharing

3.9 Information should only be shared if it is appropriate, necessary and acceptable to do so. Staff must be able to confidently identify requestors so that information is only shared with the right people. Only the minimum amount of information necessary should be shared, and should be checked for accuracy before release to avoid errors or duplicates.

3.10 All information sharing with external organisations must be governed by an appropriate information sharing agreement, and meet the requirements of the relevant legislation. All information sharing agreements must be registered with the Information Governance Department, and all data flows should be recorded on the Information Asset Register (see the Information Risk and Security Policy for details).

3.11 Information sharing within the Trust should be limited to staff who have a legitimate professional reason to access the information as part of their
contract with the Trust. Just because they work for the Trust, does not mean that they have an automatic right to access the information.

3.12 Information should only be shared via secure and authorised means, where appropriate safeguards are in place to protect the information.

**Staff Responsibilities**

3.13 All staff are required to sign appropriate data protection and confidentiality clauses to cover their work with the Trust:

- All contracted staff (substantive, permanent, fixed-term, bank, etc) are issued with a contract of employment, and non-medical staff receive a copy of the ‘Statement of Main Terms and Conditions’, both of which include appropriate data protection and confidentiality clauses. All staff are also required to sign a Data Security Statement at the time of joining the Trust, or when starting a new role (internal job changes).

- All non-contracted staff (agency, volunteers, student placements, suppliers, etc) must be engaged under an appropriate contract which contains clauses to ensure that those staff are bound by the same information governance rules as Trust staff. Non-contracted staff (all workers without a contract of employment with the Trust), must also sign a Data Security Statement on commencing work with the Trust.

3.14 To ensure that staff are effectively informed about what is required of them in relation to data protection, confidentiality and information sharing, this policy has been produced to identify the legal requirements and provide an understanding of what the Trust requires staff to do to keep personal information safe and secure. This policy is highlighted during the Trust’s induction programme, within all information governance training sessions and materials, and should be covered by line managers during local induction.

3.15 Failure to comply with data protection legislation can lead to enforcement action from the ICO, including monetary penalty notices, claims for compensation and/or criminal prosecution. It is the responsibility of every individual member of staff to be familiar with this policy (and all other related policies) to ensure the confidentiality, security and integrity of information is maintained whilst under their ownership. Any failure by a member of staff to follow the processes outlined in this policy may result in initiation of the Trust’s Staff Disciplinary Procedure.

**Records Management**

3.16 All records within the Trust must be created, maintained, retained, archived and destroyed in accordance with the [Records Management Code of Practice 2016](#). Staff must dispose of confidential information via the confidential waste bins, shredders and/or disposal bags provided.
Confidential information must not be placed in recycle or general refuse bins/areas. Confidential waste must not be used for any other purpose, e.g. as scrap paper or packing material. Please also refer to the Trust’s Corporate Records and Archiving Policy, Personnel Files Procedure or Medical Records Policy and Procedures (as appropriate).

4. DIFFERENT INFORMATION TYPES

4.1. Personal Information

‘Personal information’ is any data which can be used, directly or indirectly, to identify a person (the ‘data subject’) – “in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity” of that individual.

All information which relates to patients and staff should be treated as potentially capable of identifying the individual, and hence should be appropriately protected at all times. This includes, but is not limited to:

- demographics;
- health information;
- NHS number and hospital number;
- address and other contact information;
- photos, either digital or in printed format;
- information contained within emails;
- CCTV footage featuring the individual’s image;
- call recordings featuring the individual’s voice;
- information in a personnel file;
- National Insurance Number;
- salary/payroll and pension details.

4.2. Special Categories of Personal Information

There are also ‘special categories’ of personal information which require greater protection and justification for usage and sharing. This data is similar to ‘personal sensitive information’ previously defined under the DPA, and includes:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic and biometric data (uniquely identifying an individual),
- data concerning an individual’s health and social care; and
- data concerning an individual’s sex life or sexual orientation.
Information relating to criminal offences and convictions is no longer categorised as ‘sensitive’ under the GDPR or DPA, but there are still additional safeguards in place in relation to the processing of this data.

4.3. Confidential Information

Confidential information is anything that an individual discloses in confidence – they expect the information to be treated confidentially. This could include personal or sensitive information, but could also be commercially information about the Trust. Further information regarding confidentiality is available within Section 7 of this policy.

4.4. Audio Recordings, Photographs and Other Images

For the purpose of this policy and for clarity, any devices capable of taking still or video images will be referred to as “camera devices”. The term “images” can mean originals or copies of audio recordings, photographs and other visual images. Please see Section 9 for details.

Due to the sensitivity and confidential nature of NHS business, it is important that staff, patients, relatives and members of the public are fully aware of what images can or cannot be taken with camera devices within the Trust. This policy aims to strike a balance between the understandable desire to take legitimate images of close friends, family or colleagues, and the risks associated with unauthorised activity.

Staff must be aware of all policies relating to taking images (whether personal or care related), and patients/visitors will be made aware via advice from staff, posters placed around the Trust and other publicly available media. Advice is also available from the Information Governance Department, if required.

4.5. Closed Circuit Television (CCTV)

The processing of personal data includes any image captured by the use of CCTV. Appropriate technical and organisational measures must be undertaken by the processor of CCTV images to ensure there is no unauthorised access to the images and to secure the images from accidental loss or destruction.

Personal data may only be kept for as long as is necessary, and for its original intended purpose. Video cassettes or other storage media should therefore be cleared of footage containing personal data on a regular basis. In most cases it is unlawful to keep the images for longer than a short period and a rolling process of tape clearing/re-usage should be adopted. If footage is required as evidence of a crime, then it may be kept until after disposal of the proceedings.
The ICO has published a CCTV code of practice that must be observed by the Trust. This code is available on the ICO website: http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

5. DATA PROTECTION

5.1. Data Protection Principles

5.1.1. The GDPR is intended to strengthen and unify data protection for individuals and address the security of transferring personal data overseas. As part of this initiative, a set of revised six data protection principles define the main obligations for organisations processing personal information.

5.1.2. The new principles are similar to those in the old DPA, with added detail and an increased emphasis on accountability. The GDPR specifies that the Trust “shall be responsible for, and be able to demonstrate, compliance” with these principles. In summary, the following principles apply to all personal information:

(1) **Lawfulness, fairness and transparency** (“processed lawfully, fairly and in a transparent manner in relation to individuals”) – see Appendix B.

(2) **Purpose limitation** (“collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”)

(3) **Data minimisation** (“adequate, relevant and limited”)

(4) **Accuracy** (“accurate and, where necessary, kept up to date”)

(5) **Storage limitations** (“kept in a form which permits identification of data subjects for no longer than is necessary”)

(6) **Integrity and confidentiality** (“processed in a manner that ensures appropriate security of the personal data”)

5.1.3. The new GDPR and revised DPA do not have principles relating to individuals’ rights or overseas transfers of personal data (previously covered by principles 6 and 8 respectively under the DPA). However, these areas are separately addressed in other articles and chapters of the legislation. Further information regarding individuals’ rights can be found in the Trust’s ‘Subject Access and Other Information Rights Policy’. Additional guidance regarding overseas transfers is available in Section 10.5 of this policy. The GDPR and DPA principles are explained in full on the ICO website.
5.2. General Computer/Systems Security

5.2.1. Staff are personally responsible for maintaining the security of their Trust-issued devices (i.e. computer, laptop, ipad, iphone, etc) and the data contained on it/them, in accordance with the Trust’s IT and Information Governance policies and procedures.

5.2.2. Access to any computer/system must be password protected in line with current IT access rules and policies. Staff must not discuss with unauthorised individuals how any Trust computer or security systems operate, and should not share their login details, passwords or smartcards with anyone for any reason.

5.2.3. Computer systems should only be used to access information about individuals where there is a genuine, professional work-related reason to do so. All access to Trust computer systems is monitored and must be justified if challenged. Staff should not access the personal or confidential information of colleagues, friends or relatives (etc) if this is outside of their normal duties (as defined by their job description). Staff should not use the Trust’s computer systems to look up or update their own information, including past, present or pending medical or employment information – this should be managed formally under the Trust’s Subject Access and Other Information Rights Policy.

5.2.4. Computer screens should be out of the general/public view and should not face towards windows/doors, to ensure that personal and confidential data is only available to authorised individuals.

5.2.5. Staff should always log out of any computer system or application when work on it is finished, and ensure that the device itself is locked when not in use. PCs and laptops can be quickly locked using ‘Ctrl’+‘Alt’+‘Delete’+‘Enter’ or ‘L’+’’ on the keyboard. Mobile devices should be secured away and out of sight.

5.2.6. Information should be held on the Trust’s network servers, and not stored on local or external hard drives without explicit permission from the IT Department. Staff must not transfer any patient, staff or Trust personal or confidential information onto any personally owned (or other non-NHS) computer/electronic equipment or device without express permission from the IT and Information Governance Departments, which will only be granted in exceptional circumstances.

5.2.7. All Trust data systems must be logged on the Information Asset Register (IAR) with a named Information Asset Owner (IAO) and Information Asset Administrator (IAA) (if applicable). Further details can be found in the Trust’s Information Risk and Security Policy, and on the Information Governance pages of the intranet.
5.2.8. All staff have a responsibility to familiarise themselves and comply with the smartcard conditions of use. Members of staff with an NHS smartcard must ensure that:

- the safety and security of the smartcard is maintained;
- they do not permit another person to use the smartcard;
- they do not log into systems or software and then allow another person (whether or not they hold a smartcard) to access that system or software;
- they follow the Trust’s policies relating to smartcards.

5.2.9. When using templates (i.e. for letters, reports etc), staff must ensure that they use a ‘blank’ template; not one that has been created for another patient/client/member of staff, etc. Using templates containing another person’s details increases the risk of an error or confidentiality breach occurring.

5.3. General Security Measures

5.3.1. A Trust ID badge should be worn at all times – such as an official staff badge or other Trust-issued visitor or contractor pass. If there is any doubt about an individual’s identity, they should be challenged and the necessary evidence obtained as required – staff should be prepared to challenge people entering their work area if they do not recognise someone or if they do not have ID displayed. Further information is available from Estates/Security.

5.3.2. Cabinets, rooms and other areas containing personal and/or confidential information should be closed and locked when unattended, as far as is practically possible, and should not be accessible to unauthorised individuals at any time.

5.3.3. Information/files should be kept closed/out of sight/locked away when not in use so that the contents are not seen by unauthorised individuals. Under no circumstances should personal or confidential information be left unattended in public areas where it can be seen, read or removed by others (i.e. reception desks). Where possible, staff should adopt a ‘clear desk policy’ – please see Sections 11.1.4-11.1.5 for further details.

5.3.4. Staff must ensure that if information is being transported in any form (whether paper or electronic) it is kept secure at all times. Personal and confidential information should not be stored, transported or transferred without adequate security measures. See the Home and Off-Site/Remote Working Policy and Section 11 of this policy for further guidance on safe haven procedures.

5.3.5. Staff must ensure that confidential conversations cannot be overheard by unauthorised individuals and should not ‘gossip’
about confidential information. Please also refer to Section 7 regarding confidentiality and Section 11.6 regarding Telephones.

6. **THE CALDICOTT PRINCIPLES**

The Caldicott principles ‘mirror’ the requirements of the DPA and GDPR, and are good practice which all staff in the NHS are required to adhere to when dealing with patient identifiable information:

1. **Justify the purpose(s):** Every single proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don’t use patient identifiable information unless it is necessary:** Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s). (See Section 14 for anonymisation and pseudonymisation procedures)

3. **Use the minimum necessary patient-identifiable information:** Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to patient identifiable information should be on a strict need-to-know basis:** Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

5. **Everyone with access to patient identifiable information should be aware of their responsibilities:** Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Understand and comply with the law:** Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality:** Professionals should in the patient’s interest share information within this framework. Official policies should support them doing so.
Further information regarding the Caldicott Guardian and the Caldicott Function within the Trust can be found on the Trust’s intranet, and within the Information Governance Steering Group Terms of Reference (a copy of which is available from the Information Governance Department if required).

7. CONFIDENTIALITY

7.1 All NHS staff are bound by the terms and conditions of the Confidentiality: NHS Code of Practice (2003), which gives clear guidance on the security and disclosure of patient information.

7.2 All NHS staff also have a duty of confidence under common law when obtaining, accessing, using, holding or disposing of personal and confidential information. A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. Statute law imposes legal obligations regarding the confidentiality of patient and staff data, whether it is held manually or electronically.

7.3 All staff should be aware that it is a condition of their contract with the Trust that under no circumstances should information of a confidential nature be discussed with or passed on to any unauthorised persons at any time, either during the course of their work or outside of the working environment, whilst contracted by the Trust or after the contract has terminated. Staff should also be aware that they should not use social media, networking sites or other digital applications to discuss any aspect of their contract, or to give an opinion about patients, colleagues or the organisation. Please also refer to the Trust’s Social Networking Policy.

7.4 Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service. For guidance on sharing information with the police, please see Section 10.4 of this Policy. Further advice is also available from the relevant Safeguarding Lead and/or the Information Governance Department (as appropriate).

8. CONSENT TO THE COLLECTION, USE AND SHARING OF INFORMATION

8.1 General Conditions for Consent

8.1.1 Where the processing of personal information relies on consent (see Appendix B), the Trust must be able to demonstrate that the data subject has willingly and actively consented to the processing of their personal data. This consent must be in writing, and clearly documented/recorded in an appropriate location.
8.1.2. Consent must be given by clear affirmative action, establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of their personal data. Silence, pre-ticked boxes or inactivity (implied consent) does not constitute valid consent.

8.1.3. The consent should specify the processing activities which involve the data subject’s personal data, and where the processing has multiple purposes, consent must be obtained for each of them.

8.1.4. If the data subject’s consent is given in the context of a written declaration which includes other areas, the request for consent must be presented in a manner which is clearly distinguishable from the other areas, in an intelligible and easily accessible format, using clear and plain language. Any consent or declaration which does not meet these requirements is not legally binding.

8.1.5. The data subject has the right to withdraw their consent at any time. The withdrawal of consent will not affect the lawfulness of any processing carried out under consent before its withdrawal. Prior to giving consent, the data subject must be informed of their right to withdraw, and the process of withdrawal must be as simple and easy as providing the original consent.

Please also refer to the Trust’s “Policy for Obtaining Consent for Treatment from Adults and Children”.

8.2. Patient Information

8.2.1. The Trust’s ‘Privacy Notice’ for patients explains why data is collected, how and where it will be stored and how it will be used and shared. Patients may also be informed through information leaflets, posters, statements in patient booklets and verbally by healthcare professionals providing care and treatment. Patients should be told how their information is to be used before they are asked to provide it - or as soon as possible after.

8.2.2. Where the processing of personal information is necessary to provide a patient with health or social care or treatment, this is legally permitted under Article 6(1)(d-e) and Article 9(2)(h) of the GDPR. Separate consent is not necessary for this purpose provided that the information is not shared wider than necessary, and that ‘need to know’ principles are strictly enforced. Staff must also be aware of any duties of confidentiality which apply to the information or the circumstances (see Section 7).

8.2.3. The explicit consent of the patient must be obtained before their information is processed for any reasons other than the direct
provision of health or social care, and where this is not covered by any other legal condition in the GDPR (see Appendix B).

8.3. Information about Children and Young People

8.3.1. Where the information relates to a child less than 13 years of age and consent is required for legal processing, this must be obtained from a person with parental responsibility or other legal guardianship for the child. This authority must be verified and documented with the consent.

8.3.2. If the child/young person is aged between 13 and 18 years, it may be lawful to obtain consent directly from the data subject, however this will depend on the information being collected and the reason(s) for the processing. The Trust must be confident that the child/young person is capable of understanding the request and providing informed consent. It may still be appropriate to obtain consent from a person with parental/legal responsibility.

8.4. Information about Individuals Lacking Capacity

8.4.1. Where the information relates to an individual who lacks capacity and consent is required for legal processing, this must be obtained from a person with legal responsibility for the data subject – for example, someone with the appropriate power of attorney. This authority must be verified and documented with the consent.

8.5. Staff Information

8.5.1. As part of its responsibilities as an employer, the Trust will collect, process and share information about its staff, which is legally permitted under Article 6(1)(e) and Article 9(2)(b) of the GDPR.

8.5.2. The Trust’s ‘Privacy Notice’ for staff explains why the data is collected, how and where it will be stored and how it will be used and shared. This is referred to within the ‘Statement of Main Terms and Conditions’ and ‘Personal Profile’ which is issued to all staff. The privacy notice is available on the Trust’s public website and is included on all job adverts and displayed in key locations.

8.5.3. The personal information of staff, such as name and job role, may also be collected and used by the Trust as part of its duties as a public organisation – for example, as part of meetings or within policies. This is legally permitted under Article 6(1)(e) of the GDPR.

8.5.4. The explicit consent of staff must be obtained before their information is processed for any reason(s) not covered by any other legal condition in the GDPR (see Appendix B).
9. IMAGES, AUDIO AND VIDEO – CLINICAL AND NON-CLINICAL USE

9.1. Definitions and General Principles

9.1.1. The term “images” is used in this policy to collectively refer to all media types, including originals and copies of audio recordings, photographs and other visual images, such as x-rays and MRI scans. For the purpose of this policy, any devices capable of taking still or video images (including mobile phones and tablets) will be referred to collectively as “camera devices”.

9.1.2. Staff must ensure that the authorised use of camera devices and images for all clinical and non-clinical purposes is carried out with due regard for the rights of all patients, staff, visitors and members of the public. The Trust upholds the right of an individual to appropriate care, balanced with privacy and confidentiality.

9.1.3. Staff should not use their personal camera devices to take any type of medical/clinical image for any purpose without explicit permission from the Information Governance Department (which will only be given in exceptional cases).

9.1.4. Depending on the purpose (and content) of the image required, written consent may not be required from the individual:

9.1.5. Please also refer to the Trust’s ‘Policy for Obtaining Consent for Treatment from Adults and Children’. Additional guidance is available from health professional bodies.
9.2. Clinical Purposes

9.2.1. Images made for clinical purposes form part of a patient’s medical record, and therefore the processing of this information is legally permitted under Article 9(2)(h) of the GDPR. Separate consent is not required for this purpose; however staff should always ensure that patients are aware of the reason(s) for the image, and that it will be retained within their medical record. Images obtained for clinical purposes should not be used for any other purpose without explicit consent (see 9.3 below).

9.2.2. Certain images will be taken by specific departments, such as X-Ray, Radiology and Ultrasound. Other images can be requested via the Medical Photography Department, or may be taken by a ward/department using a Trust-approved camera device. All images should be uploaded into the patient’s EPR record.

9.3. Clinical Images for Non-Clinical Purposes

9.3.1. Clinical images of patients can only be used for non-clinical purposes (such as research and training) with explicit consent from the individual. The only exception to this is if the images are fully anonymised and have no ability to identify the specific individual to whom they relate. Particular care should be taken when an anonymised image may still have the potential to identify an individual (for example, where a rare condition is clearly visible).

9.3.2. When clinical images of patients are required for non-clinical purposes, the accountability and responsibility for the use of the images rests with the requesting member of staff, as does the requirement to obtain appropriate consent. Where images are requested from the Medical Photography archive, these will not be released without evidence of appropriate consent.

9.3.3. The standard images consent form should be signed by the patient (or their carer, representative, parent or guardian, as applicable – see Section 8). The signed consent form should be uploaded into EPR with the images, and a copy given to the signatory. The template consent form is available on the intranet.

9.4. Media and Other Promotional Use

9.4.1. From time to time, the Trust seeks to promote the services that it provides and raise awareness of good-news stories and achievements. This may be through in-house managed platforms, such as newsletters, the public website and social media, or via external organisations such as journalists, broadcasters and in professional or medical journals or publications. Images
taken/obtained by the Trust may only be used for this purpose with the explicit permission of the individual to whom they relate.

9.4.2. The standard images consent form should be signed by the individual (or their carer, representative, parent or guardian, as applicable – see Section 8). The template consent form is available on the intranet. The signed consent form should be retained by the person taking the image, and a copy given to the signatory. It is the responsibility of the ward/department to manage the storage of the media and relevant consent forms. These must be stored centrally on the network (not local PCs or devices) with appropriate access to relevant staff for audit and reference purposes.

Further guidance on media usage is available on the ICO website: https://ico.org.uk/for-organisations/media/

9.5. Personal Photos

It is appreciated that relatives and visitors of patients may wish to take photos of their loved ones whilst they are in hospital. Staff may also have a desire to take images of themselves or colleagues in the work environment for personal reasons, such as updates on private social media profiles. In addition to the requirements of the Trust’s Social Media Policy, there are some conditions for allowing this practice:

9.5.1. Images should be restricted to non-clinical areas (such as corridors, waiting rooms or outside). Images can only be taken in clinical areas (such as wards and treatment rooms) with the express permission of a senior member of staff.

9.5.2. Consideration should be given to the appropriateness of the image (i.e. the condition or portrayal of the individuals in shot, and their surroundings). If there is any doubt, the request should be discussed with a senior member of staff or the Information Governance Department.

9.5.3. Images must be limited to the person/people they are aimed at (such as the patient and their relative) and should not include any other individuals without their explicit permission. Images should not be taken of an unconscious patient without the express permission of a senior member of staff and a justifiable reason for taking the image.

9.5.4. Images should not be uploaded to social media or other networking sites without explicit permission from all individuals included within the image. Providing consent to have the image taken does not give automatic consent for sharing of the image. Please refer to the Trust’s Social Media Policy. If the image has
been specifically taken for official media usage by the Trust, explicit written consent is required - please see section 9.4.

9.5.5. If an image has been taken or used inappropriately or without permission, the individual should be asked to permanently delete the image, and provide evidence that this has been actioned. Where deletion/removal is refused, this may result in legal action and/or disciplinary action in the case of staff. Any abuse of images should be immediately reported to the Information Governance Department and formally logged in Datix.

10. INFORMATION SHARING

10.1. Principles of Information Sharing

10.1.1. The sharing of any personal or confidential information should be governed by a balance between clear rules which satisfy the requirements of law and guidance, and the encouragement of efficient working practices in both the disclosing and receiving organisations. The Trust will endeavour to have mechanisms in place to ensure that:

- patients are aware of who the Trust’s information sharing partner agencies are (see section 2.4);
- consent is obtained as appropriate (see section 8); and
- there are regular reviews of our information transfers.

10.1.2. Individuals’ rights regarding the sharing of their personal information are supported by the NHS Care Record Guarantee, which sets out high-level commitments for protecting and safeguarding service user information. Particularly in relation to individuals’ rights of access to their own information, how information will be shared (both internally and externally) and how decisions on sharing information will be made.

10.1.3. The NHS Constitution sets out a series of patient rights and pledges which all NHS organisations are required by law to take into account as part of their decisions and actions. This includes an individuals’ “right to privacy and confidentiality, and to expect the NHS to keep [their] confidential information safe and secure.”

10.1.4. The Trust will endeavour to ensure that all information transfers in or out of the organisation are protected by appropriate information sharing protocols and that the receipt and transfer of all personal sensitive and Trust confidential information occurs within the boundaries of this policy and associated procedures. Please also refer to section 11 regarding Safe Haven procedures.
10.2. Information Sharing for Care Purposes

10.2.1. Health and social care professionals should have the confidence to share information in the best interests of their patients/service users within the framework set out by the Caldicott Principles (see section 6). The primary concern must be for the health and wellbeing of the individual receiving direct care, and a failure to share information (both efficiently and securely) may have serious consequences for patient/service user welfare.

10.2.2. Where a patient’s care or treatment is transferred to another NHS organisation, the record may be transferred directly with the patient themselves (if the transport is coordinated by the Trust) or via a request from the other organisation to the Trust’s Medico-Legal Department. As the sharing of this information forms part of the patient’s ongoing healthcare, this is legally permitted under Article 6(1)(d-e) and Article 9(2)(h) of the GDPR and separate patient consent is not required. However, the referring clinician must ensure that the patient is aware of the information sharing. Where a patient chooses to seek care or treatment from a private organisation, information will only be shared by the Trust with explicit written permission from the patient. Further guidance is available within the Trust’s Subject Access and Other Information Rights Policy.

10.2.3. Wards and departments must ensure that systems are in place to support coordinated care through clear and accurate information exchange between relevant health and social care professionals, both internal and external to the Trust, as appropriate to a patient’s health and social care and treatment.

10.2.4. Staff should ensure that systems are in place to establish, respect and review patients’ preferences for sharing information with partners, family members and/or carers (also see section 8 regarding Consent and section 11.6 for additional guidance regarding telephone requests for information).

10.2.5. If there are any concerns about barriers preventing appropriate information sharing, this should be discussed with a senior member of staff or the Information Governance Department.

10.3. Information Sharing Agreements/Protocols/Contracts

10.3.1. Personal and confidential data may only be shared outside of the Trust where there is legal justification or explicit consent from the data subject. All information sharing with organisations outside of the Trust must be governed by an appropriate information sharing protocol, commercial contract, service level agreement or other appropriate legal documentation, which includes robust
information governance clauses/arrangements. This includes sharing with other NHS organisations, unless the sharing is a direct result of a transfer of, or referral for care (see 10.2.2).

10.3.2. The Trust is a signatory to the Dorset Information Sharing Charter and other similar local protocols (See 2.4), which provide the overarching principles to encourage the appropriate sharing of information between agencies for the purpose of providing health and social care services to patients. However, this does not overrule the need to have specific information sharing protocols in place when there is sharing of information between organisations. The local protocols simply provide high level sharing principles, and a commitment to collaborative working.

Further guidance regarding information sharing agreements is available from the Information Governance Department.

10.4. Disclosure of Information to the Police

10.4.1. Data protection legislation allows for personal data to be disclosed to the police in order to assist in “the prevention or detection of crime” and/or “the apprehension of prosecution of offenders”. Section 115 of the Crime and Disorder Act 1998 also allows the sharing of information to “relevant authorities” (for example: the police, local authorities, health authorities, and local probation boards), “where the disclosure is necessary or expedient for the purposes of any provision” of the Act.

10.4.2. If the individual who is the subject of the request is available and capable, they should be asked to provide their explicit, written consent for the Trust to disclose the information requested, unless this would prejudice the enquiry or court case. For the Trust to consider releasing any information without consent, the request must relate to a serious crime (under the Crime and Disorder Act 1998), otherwise the Police should be asked to obtain a Court Order or written signed consent.

10.4.3. All requests from the police should be submitted in writing (electronic or hard copy), ideally presented on an official DP2, C399, MG11 or A232 form (see intranet for details). Requests may be dealt with by the Information Governance Department, the Medico-Legal Department or a specific ward/department, such as A&E, depending on the nature and subject of the request.

10.4.4. If there is any doubt about releasing information to the police, advice should be sought from senior management and/or the Information Governance Department before any disclosure is made. A copy of the Police request, the decision made and any information supplied must be recorded on the individual’s file.
Further guidance is also available in the Trust’s Medical Records Policy and Personnel Files Procedure, and advice can be sought from the Information Governance Department if required.

10.5. Transfers Outside of the European Economic Area (EEA)

Chapter V of the GDPR imposes restrictions on the transfer of personal information outside the European Union (EU) in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal information may only be transferred outside of the EU where the receiving organisation has provided sufficient evidence of adequate safeguards. Should there be a requirement to transfer personal information outside of the EU, this should be discussed with the Information Governance Department, and a privacy impact assessment should be completed to review the associated risks and available safeguards.

10.6. Freedom of Information (FOI) Requests

Where an organisation uses public money, the Freedom of Information (FOI) Act 2000 puts a duty on that organisation to provide information to individuals who make a written request for it. There is a list of exemptions which prevent the release of certain information – such as personal and confidential information which identifies individual staff or patients. All FOI requests are coordinated via the Information Governance Department to ensure that only appropriate information is released and shared. This process is governed under the Trust’s Freedom of Information Policy.

11. SAFE HAVEN PROCEDURES (INFORMATION SHARING)

11.1. What is a “Safe Haven”?

11.1.1. “Safe haven” is a virtual concept used to describe an agreed set of arrangements and safeguards that are in place to ensure that personal and confidential information can be communicated safely and securely. The term was original used to cover the transfer of information by fax, but now it also covers all data held, used and transferred by post, telephone/answerphone, digital and manual records, white/notice boards, email, and bulk data transfers (51 records or more). Every member of staff is personally responsible for taking precautions to ensure the security of information, using the most up to date, reliable and approved forms of data transfer.

11.1.2. The Trust will endeavour to ensure that all locations on-site where personal or confidential information is received, held or communicated are deemed as safe havens. These designated safe havens will use a combination of measures (physical, electronic and personal) to protect information, and the best
Data Protection and Information Sharing
Document No: IG.P01
Version No: 3.2(FINAL)

practice principles described in this policy should be applied to all incoming and outgoing information flows to ensure that they are secure, justifiable and proportionate.

11.1.3. The clear priority is that members of the public and visitors to the Trust do not gain access to any area of the Trust deemed as a safe haven. Any physical safe haven locations should be locked or accessible via a coded key pad (or other robust locking mechanism), the code/key for which is only known/accessible to authorised staff; or, it should be sited in such a way that only authorised staff can enter. If located on the ground floor, any windows should have locks on them which are used accordingly. The area should conform to health and safety requirements in terms of fire, safety from flood, theft and environmental damage.

11.1.4. The Trust also operates a clear desk policy in order to:

a) support the security of personal and confidential information;

b) ensure a professional image of the Trust is presented to patients, visitors and other staff; and

c) encourage a reduction in the amount of paper used by staff.

Scientific studies have also shown that having a clear desk reduces stress, as well as helping to minimise accidents and spills.

11.1.5. At the end of the working day, staff are expected to tidy their desk/workspace and to clear away all hard copy records. Mobile devices should not be left on display or accessible to unauthorised individuals. It may also be appropriate for hard copy records and mobile devices to be put into a locked cabinet/drawer/etc. PCs must be switched off, or logged out if continued use is required by other authorised individuals.

11.2. Emails/Electronic Information

11.2.1. Personal or confidential information should only be sent via email if it is appropriately encrypted. Only official NHS-issued email accounts should be used to send or discuss personal or confidential information. Personal/home email addresses should never be used by staff for any Trust business.

11.2.2. Where the email is sent from a ‘poole.nhs.uk’ account to a domain included on the IT secure list (see intranet for details), the email and any attachments will be automatically encrypted. This is also the case for emails sent between ‘NHS.net’ accounts. Emails sent to any other address should be manually encrypted by including “[SECURE]” in the subject line of the email.
11.2.3. Personal and confidential information must not be transmitted via the internet without it being encrypted, or where system-to-system networks are known to be secure. Where online submissions are required, this should be discussed with the IT Department first. Further guidance regarding emails and electronic transfers is available in the Trust’s Informatics Policies.

11.2.4. Dictation machines and tapes can contain extremely sensitive information and should always be held securely and kept in a locked area when not in use. They should be cleared of all dictation when the content has been completed/processed.

11.2.5. Where possible, photocopying/scanning machines should be sited in areas away from the general public, and must have the secure-printing function enabled. Care should be taken by staff to ensure that paper is not left on the glass after copying and all printing and copying is collected without delay. Staff must ensure that they have the correct printer selected when sending information to print to avoid confidential or personal data becoming inappropriately available to others.

11.3. Removable Media (USB Sticks/CDs/DVDs/etc)

11.3.1. Personal and confidential information should not be stored on removable media unless absolutely necessary. If you have a requirement to use removable media, you should discuss the available options with the IT Department.

11.3.2. Where the use of removable media is required and approved:

a) the information should only be retained on the device for the minimum period possible (the information should be backed-up to networked storage if it is to remain on the device for more than a simple transfer between Trust systems);
b) only a Trust-approved device, encrypted to nationally approved standards, should be used (unless authorised by both the IT and Information Governance Departments); and

c) the physical security of the device must be protected.

11.4. Faxing

11.4.1. In support of NHS England’s desire to cease “the outdated use of fax machines”, the Trust does not encourage faxing as a method of transfer for the same reasons of safety and efficiency.

11.4.2. Personal and confidential information must only be sent by fax where it is absolutely necessary to do so, and there is no alternative method of transfer. The use of secure email should always be considered first before sending information by fax.

11.4.3. Where it is absolutely necessary to send a fax message, this should be sent using the safe haven procedures described below:

a) The fax should be sent to a safe haven location where only individuals that have a legitimate right to view the information can access it. Confidential faxes, both incoming and outgoing, must not be left where unauthorised people may see them.

b) Faxes sent must include a cover sheet, which is marked ‘Private and Confidential’ and contains a suitable confidentiality clause (a template is available on the intranet).

c) The sender must be certain that the correct person will receive the fax. The recipient must be notified when the fax is being sent and should be asked to acknowledge receipt. If possible, a report sheet should be produced to confirm successful transmission.

d) Staff should ensure that the fax number is correct and take care when dialling. Where possible, pre-programmed numbers should be used (and regularly checked for any changes).

e) Only the minimum amount of personal and confidential information should be included in the fax message. Where possible, the information should be anonymised or pseudonymised (see Section 14 for more details).

11.4.4. If a document is incorrectly received within the Trust, it is the receiving ward/department’s responsibility to ensure that it is given to the named recipient and/or the sender is notified of the error. The error should also be logged in Datix.
11.4.5. When installing fax machines, consideration should be given to any security tools available on the machine, such as password protected memory. If the room/area containing the machine cannot be locked overnight/when the area is unattended, machines should either be turned off or moved to a secure/locked office or cupboard.

11.5. Mailing/Posting/Courier

11.5.1. Care must be taken to ensure that both internal and external mail is addressed correctly and is packaged appropriately.

11.5.2. In public areas, incoming mail should be opened away from public view, stored face down and not left unsupervised.

11.5.3. Envelopes containing personal or confidential information must be securely sealed, addressed to a specific individual and clearly marked “private and confidential” and/or “for addressee only”. External mail is automatically marked as sent from the Trust when franked by the post room, indicating a return address if required.

11.5.4. Care should be taken by staff to ensure that envelopes do not contain information which is not intended for the recipient. For example, inadvertently picking up two patients’ letters instead of one and sending them to the same address. This can result in a serious breach of patient confidentiality and could lead to serious consequences for the Trust and the individual staff involved.

11.5.5. When sending highly sensitive or confidential information, careful consideration should be given to the method of transport and the suitability of packaging material. When sending by external mail, this must be via a secure method where the package can be traced and is signed for on receipt.

11.5.6. The internal mail should be avoided when sending highly confidential information – this should be hand-delivered where possible. When transporting personal or confidential information by hand, it must be appropriately secured (for example, placed in a non-transparent envelope or lockable case) to avoid information being lost or inappropriately visible.

11.5.7. Only companies that hold an existing contract/SLA with the Trust (with appropriate information governance clauses) can be used to transport patients, staff, equipment or documentation. Any personal or confidential information transported in this way should be signed in and out appropriately and copy evidence of sending/receipt retained. Further advice is available from the Logistics and Transport Departments.
11.6. Telephones/Answer Machines/Messages/Verbal Conversations

11.6.1. Staff are expected to apply common sense with regard to the location used for highly confidential telephone calls or discussions. For example, using a private office instead of an open plan area, and not playing received answerphone messages on speakerphone in public areas or locations where there is a risk that they could be overheard by unauthorised individuals.

11.6.2. The contact information of individual staff must never be given over the phone unless that member of staff has authorised its release, or it is already within the public domain. This includes Trust email addresses and extension numbers.

11.6.3. When speaking with individuals over the telephone, it is important to confirm their identity before any personal or confidential information is disclosed. Staff must also ensure that the individual has a right to access the information. If the individual’s identity cannot be verified and/or the member of staff dealing with the call is uncomfortable with releasing information over the telephone, no information should be released.

11.6.4. Staff must be aware of issues surrounding patients whose electronic healthcare record has been marked with a Critical Patient Information (CPI) flag or EPR alert showing the need for anonymity protection or additional safeguards. Any caller wanting information on a flagged patient should be put on hold and immediate advice sought from senior management.

11.6.5. When dealing with incoming calls, staff may need to apply different safeguards depending on the type of information being requested and who the caller claims to be:

   a) OUTPATIENTS/INPATIENTS: Personal information relating to outpatients should only be disclosed to the patient. For inpatients, all calls are directed to the ward / department where the patient is located unless there is a CPI flag or EPR alert preventing this. Therefore, it is imperative that any special circumstances regarding an inpatient’s circumstances are appropriately raised and recorded.

   b) THE PATIENT: Before releasing any information to a caller who claims to be patient, staff should ensure they gain assurance of the caller’s identity by obtaining confirmation of certain personal details, for example: Date of birth, address and post code, appointment dates, treatment / clinic details, hospital or NHS number. A patient may choose to apply an additional safeguard to their medical record by insisting that a password
they have set up is provided by any caller before any information is released.

c) **NEXT OF KIN:** Information should only be disclosed to next of kin, relatives or friends when the consent of the patient has been obtained. It is important to note that next of kin do not have any automatic right to access confidential patient information. Parents / those with parental responsibility have a right to information about their children, unless the child has sought treatment independently of their parents (see section 7 on confidentiality and section 8 regarding consent).

d) **RELATIVES/REPRESENTATIVES:** As part of the admission process, patients may be asked in advance whether they wish for information about their care to be shared with any named individual. Information may then be shared with that individual, either in person or over the phone, without the need to gain further consent. Where a named representative is confirmed, their contact details should be recorded on the patient’s electronic and manual records to ensure the patient’s wishes are consistently followed.

e) **OTHER THIRD PARTIES:** Where other individuals (e.g. health and social care providers, the police, local authorities, etc) request information about a patient, you must be able to confirm the caller’s identity and see evidence that they are authorised to receive the information (such as the patient’s consent, legal authorisation, etc.).

11.6.6. A patient’s right to privacy means that when making outgoing calls, we need to speak to the patient directly, unless we have specific consent from the patient or it is justifiable to speak to someone else. Wherever possible, patients’ should be asked in advance if they have any preferences, and these should be centrally recorded and regularly checked for updates/changes. For example: Would they prefer to be called at work or home? Would they like information to be left with a family member if they know they cannot be contacted directly? Are they happy for voicemail messages to be left?

11.6.7. When leaving answerphone messages for patients, there is a balance to be struck between respecting the privacy of the patient, not unduly worrying them with an obscure message, and ensuring that the recipient understands that it is a genuine message (e.g. not a scam that is looking to get them to call back a premium rate number). Staff should take responsibility for considering whether any particular privacy issues exist that could affect whether it is appropriate to leave an answerphone message. For example, staff should consider the following:
• Have the patient’s preferences been followed? (see 11.6.6)
• Who else might hear the message?
• Has the correct number been dialled?
• Will the patient fully understand the content of the message?
• Can you be certain the message will be received?
• Is there a risk of breaching the patient’s confidentiality?

Further guidance on the release of information by telephone can be found in the Medical Records Policy and Procedures on the intranet.

11.7. Whiteboards and other visual aids

11.7.1. Whiteboards (and similar other visual aids such as notice boards, TV and PC screens) are used all around the Trust to support with the effective delivery of our services. However, when displaying information which may be seen by individuals such as visitors, patients or the general public, it is important that confidentiality is not compromised by displaying too much information.

11.7.2. All patient details (clinical and non-clinical), must be handled in such a way as to remain confidential between the Trust and the patient. As well as having information governance implications, there are safeguarding issues to consider.

11.7.3. Where a whiteboard, notice board or other visual aid is used in an area where it is on open view to the public or in a prominent position, it must not be used to display any personal or confidential information where this can be used to identify an individual. Where no other suitable location is available, only the minimum amount of information should be displayed and appropriate safe haven procedures must be in place to protect the information without compromising clinical or patient needs. For example, where boards are used to monitor patient locations/consultants/conditions (etc) on a ward: only use the patient’s initials, not their full name; you can indicate that an alert exists for a patient, but do not display details of the alert; etc.

11.7.4. These principles also apply to staff information, such as rota and annual leave details – this information should not be on display in public areas, or in a way which makes the information accessible to unauthorised individuals. Where photos of staff are displayed on public notice boards as an introduction to the ward or team, then this is acceptable provided that the individual member of staff has consented to this (see Section 9).

11.8. Remote Working (Home, Off-Site, Community, etc)

11.8.1. Staff are responsible for the confidentiality and security of any information that they hold remotely, either in paper or electronic
format, and for its transportation to and from Trust premises. Staff should ensure they hold only the minimum level of confidential information remotely, and ensure compliance with the relevant Informatics and Information Governance policies.

11.8.2. An IG Questionnaire must be completed prior to any home or off-site/remote working to advise the Information Governance Department of the proposed arrangements and enable them to provide appropriate support to minimise any risks associated with potential issues relating to data protection and confidentiality.

For further details and guidance regarding remote working, please refer to the Trust’s Home and Off-Site/Remote Working Policy.

12. USING INFORMATION FOR TRAINING, RESEARCH AND AUDIT PURPOSES

Additional advice and guidance is also available online via the GMC website: https://www.gmc-uk.org/guidance/ethical_guidance/30660.asp

12.1. Students, Trainees and Honorary Placements

12.1.1. If a student, trainee or honorary clinician/healthcare provider is included within the healthcare team providing (or supporting) a patient’s care, they can have access to the patient’s personal information like other team members, unless the patient objects.

12.1.2. Patients must be asked to provide their consent to allow a trainee or student to sit in on any medical consultation. It is the lead clinician’s responsibility to ensure that the patient is under no pressure to consent, and that the trainee/student’s presence does not adversely affect the patient’s care.

12.2. Training and Education

Most patients understand and accept that health education and training relies on having access to information about patients and medical conditions. For most of these purposes, anonymised information will be sufficient and should be used whenever practicable. If information or media is used which can (directly and or indirectly) identify an individual, then explicit consent must be obtained. See Section 8 of this policy regarding consent.

12.3. Research and Clinical Audits

The Trust will endeavour to ensure that systems of authorisation for research projects are in place and that local ethical and audit committees are aware of the responsibilities of clinical staff and researchers in relation to confidentiality and the promotion of good
practice. Further guidance is available from the Research & Innovation and Clinical Audit Departments, as appropriate.

13. USING INFORMATION FOR SYSTEM TESTING AND TRAINING

13.1. There are a number of risks that exist whenever system testing or training is undertaken using live data or a live environment, including unauthorised access to or disclosure of data and/or corruption or loss of data. These risks can also lead to financial loss to the Trust and/or the person to whom the information relates.

13.2. The ICO advises that the use of personal data for system testing/training should be avoided. Where there is no practical alternative to using live data for this purpose, system administrators should develop alternative methods of system testing/training. Before commencing any system testing/training using live data, staff must undertake a Privacy Impact Assessment (PIA). If the ICO were to receive a complaint about the use of personal data for system testing/training, their first question to the Trust would be to ask why no alternative to the use of live data had been found and how we documented the risk assessment and decision taken.

13.3. For general staff training purposes, live data should not be used as a dataset without explicit consent from the data subject. Fictional, convincing information is the most appropriate dataset to be used, where no real person can be identified from the information used.

13.4. Where personal or confidential information has the potential to be used for training purposes in the future, the individual must be informed at the time of collecting the data and appropriate consent obtained (see Section 9). For example, if telephone calls are recording for training and monitoring purposes, it may be proportionate to use a recording of a conversation to review how it went, in order to identify training needs with the staff member involved, as long as the data subject has been informed as above. No recording or use of a transcript of a call or conversation may be used for wider training unless we have explicit permission from the data subject – the fact that a person has not objected to the recording itself is not good enough for this purpose.

14. PSEUDONYMISATION AND ANONYMISATION

14.1. Pseudonymisation

14.1.1. Pseudonymised information is where an individual’s identity is disguised by using a unique identifier (a pseudonym). The pseudonym does not reveal an individual’s ‘real world’ identity, but allows the linking of different data sets for the individual concerned. Pseudonymised data is still classed as identifiable data and should be handled as such, and must only be transferred using secure means.
14.2. Anonymisation

14.2.1. Anonymised information does not identify an individual and cannot be reasonably used to determine their identity. Anonymisation requires the removal of any detail, or combination of details, that might enable identification, either by itself or when used with other available information (see 14.3).

14.2.2. Effectively anonymised information (where the prospect of identifying individuals is remote), is not seen as personal data and therefore data protection rules do not apply.

14.2.3. It is generally acceptable for anonymised information to be used or disclosed without the data subject’s consent, as the information can no longer be used to identify a specific individual. However, the anonymisation must be done effectively (see 14.3 below), and neither the anonymisation process, nor the use of the anonymised information, should have any direct detrimental effect on any particular individual.

14.3. Risk of Re-identification

14.3.1. To ensure that effective pseudonymisation or anonymisation has been applied, a 'motivated intruder' test should be undertaken. This checks whether a reasonably competent individual who wished to de-anonymise data could successfully do so. Further guidance on conducting this test and the steps to follow is available within the ICO Anonymisation Code of Practice: https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

14.3.2. There are cases where it will be difficult to determine whether there is a reasonable likelihood of re-identification taking place. For example, it is difficult to determine the risk of re-identification of pseudonymised data sets, because even though pseudonymised information does not identify individuals to those who do not have access to the ‘key’, the possibility of linking several pseudonymised datasets to the same individual can be a precursor to identification. Any concerns regarding re-identification should be discussed with the Information Governance Department before any information is released.

14.4. Secondary Uses of Patient Information

14.4.1. Patient information is collected for the purpose of delivering health and social services to the individual. This is known as 'primary use' (or direct healthcare purposes), and also includes relevant supporting administrative processes and audit/assurance of the quality of services provided. 'Secondary use' refers to the
use of patient information for non-direct healthcare purposes, such as research, audits, commissioning and reporting.

14.4.2. The principles of pseudonymisation and anonymisation apply to the use of patient information for secondary use. Through de-identification, users are able to make use of individual data for a range of secondary purposes without having to access the identifiable data items.

14.4.3. Staff must only have access to the data that is necessary for the completion of the business activity they are involved in. This is reflected in the Caldicott Principles (‘need to know’ access) and extends to both primary and secondary uses.

14.4.4. For direct healthcare purposes, the use of identifiable data is required to ensure patient safety. Under data protection legislation, the Trust is permitted to use patient information for the purposes of preventative or occupational medicine, medical diagnosis, the provision of health or social care or treatment, and the management of health or social care systems and services. The use of identifiable patient data for secondary purposes must have legal justification and/or explicit written consent:

   a) A number of non-direct healthcare purposes will routinely be conducted with explicit patient consent. For example: consent for staff to access information for the purpose of investigating a complaint, or consent for a third party (solicitors, other family members etc) to be given access to data as part of a subject access request.

   b) Existing legislation provides support for a number of non-direct healthcare purposes. For example: the DPA includes provision for the Trust to disclose data without consent to the police in certain circumstances (see section 10.4 for details).

   c) There are regulations in place relating to specific organisations, such as the Care Quality Commission (CQC) or Health Protection Agency (part of Public Health England), which support the use of identifiable data for some non-direct healthcare purposes relating to their regulatory function. For example: Under section 63(2)(b) of the Health and Social Care Act 2008, a person authorised to carry out an Inspection on behalf of the CQC may access, inspect and take copies of any documents or records held by the Trust, where they consider it ‘necessary or expedient’ to do so for the exercise of CQC’s ‘regulatory functions’.

   d) Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001) allows the common law duty of confidentiality to be set aside in specific
circumstances where anonymised information is not sufficient and where patient consent is not practicable. This is managed by the Confidentiality Advisory Group.

14.4.5. All organisations that process personal information are required under data protection legislation to protect it from inappropriate disclosure. Effective pseudonymisation and anonymisation techniques enable the Trust to undertake secondary use in a safe, secure and legal way. By removing identifiable data, it allows the Trust to share or publish more information with fewer restrictions.


15. IMPLEMENTATION AND REVIEW

15.1. Consultation and Implementation

15.1.1. This policy has been drafted by the Information Governance Department in accordance with the Trust's statutory obligations and responsibilities under the relevant legislation.

15.1.2. This policy will be ratified by the Information Governance Steering Group (IGSG) prior to launch, publication and use within the organisation. In accordance with the IGSG Terms of Reference, minutes from all IGSG meetings are reviewed by the Hospital Executive Group (HEG).

15.1.3. All policies are published on the staff intranet and communication is circulated to all staff when new policies or changes to existing policies are released. Staff will also be made aware of existing policies, procedures and legislation via annual IG training.

15.2. Policy Review Arrangements

15.2.1. This policy will be reviewed by the Information Governance Department on at least a three-yearly basis. An earlier review may be instigated where there is a change in legislation or practice, or new guidelines are published which impact on the particulars of this policy.

15.2.2. Any major updates or changes to this policy will be ratified by the Senior Information Risk Owner, Caldicott Guardian and/or the IGSG (as appropriate) prior to implementation. The application and use of this policy will be monitored by the Information Governance Department and IGSG as part of its formal arrangements.
15.3. Monitoring Effectiveness

15.3.1. All areas of the Trust are required to complete an annual Information Risk and Security Audit to demonstrate their compliance against current policies and procedures. These audits will highlight if any information has been put at risk through deliberate/inadvertent misuse of systems (electronic and paper), or as a result of weak, non-existent or poorly applied controls. All completed audits are reviewed by the Information Governance Department, and follow-up action taken as necessary. Audit statistics are provided to the IGSG on a regular basis.

15.3.2. The Trust will also monitor the effectiveness of this policy via the use of Privacy Impact Assessments and the review of incidents and near-misses recorded within the Datix system. Please refer to the Information Risk and Security Policy for further details.
APPENDIX A: EQUALITY IMPACT ASSESSMENT

<table>
<thead>
<tr>
<th>Date of Assessment</th>
<th>April 2014 / Nov 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessor Details</td>
<td>Information Governance Officer</td>
</tr>
</tbody>
</table>

**Assessment Area**
Data Protection and Information Sharing Policy (previously the separate ‘Data Protection and Confidentiality’ and ‘Information Sharing’ policies)

**Purpose, Aims and Intended Outcomes**
See Sections 1 and 2 of the policy for details regarding the purpose, aims and intended outcomes of the policy.

**Target Group(s) and Impact/Influence**
This policy is applicable to all staff and there is no anticipated detrimental impact on any equality group. This policy makes all reasonable provision to ensure equal access to all staff. There are no statements, conditions or requirements that disadvantage any particular group of people.

**Assessment of Aspects/Activities Relevant to Equality**

<table>
<thead>
<tr>
<th>Accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>All IG policies and guidance are accessible for all managers and staff via the intranet and copies are obtainable from the IG Team.</td>
</tr>
</tbody>
</table>

**Consultation and Communication**
This policy will be ratified by the IGSG prior to launch, publication and use within the organisation. All policies are communicated widely and openly across the organisation, will be accessible to everyone via the intranet and as required staff will be supported in their application of the policy.

**Implementation**
The application of this policy supports the Trust’s duties under the Equality Act 2010. The organisation will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity and provide for good relations between all people of all diverse groups.

**Monitoring and Review**
This policy will be reviewed by the IG Department on at least a three-yearly basis, unless there is a change in legislation or practice, or new guidelines are published which necessitates an earlier review. Any major updates or changes will be ratified by the SIRO, Caldicott Guardian and/or IGSG prior to implementation. The application and use of this policy will be monitored by IG and the IGSG as part of its formal arrangements.
**APPENDIX B: PROCESSING CONDITIONS FOR PERSONAL INFORMATION**

For processing of personal information to be lawful, we must identify a legal basis, sometimes referred to as the “conditions for processing”. It is important to determine, and also document, the legal basis for processing personal data. This becomes more of an issue under the GDPR because the legal basis for processing can have an effect on an individual’s rights. Below are the legal bases available for processing personal (and special categories) of information under data protection legislation:

### Legal conditions for processing PERSONAL information

| (a). | Consent of the data subject. |
| (b). | Processing is necessary for the **performance of a contract** with the data subject or to take steps to **enter into a contract**. |
| (c). | Processing is necessary for **compliance with a legal obligation**. |
| (d). | Processing is necessary to protect the **vital interests** of a data subject or another person. |
| (e). | Processing is necessary for the performance of a task carried out in the **public interest** or in the **exercise of official authority** vested in the controller. |
| (f). | Necessary for the purposes of **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.) |

### Legal conditions for processing SPECIAL CATEGORIES of personal information

| (a). | **Explicit consent** of the data subject, unless reliance on consent is prohibited by EU or Member State law. |
| (b). | Processing is necessary for carrying out **obligations under employment, social security or social protection law**, or a collective agreement. |
| (c). | Processing is necessary to protect the **vital interests** of a data subject or another individual where the data subject is physically or legally **incapable of giving consent**. |
| (d). | Processing carried out by a **not-for-profit body** with a **political, philosophical, religious or trade union aim** provided the processing relates only to **members or former members** (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent. |
| (e). | Processing relates to personal data manifestly **made public by the data subject**. |
| (f). | Processing is necessary for the establishment, exercise or defence of **legal claims** or where courts are acting in their **judicial capacity**. |
## Legal conditions for processing SPECIAL CATEGORIES of personal information

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(g)</td>
<td>Processing is necessary for reasons of <strong>substantial public interest</strong> on the basis of Union or Member State law which is proportionate to the aim pursued and which contains <strong>appropriate safeguards</strong>.</td>
</tr>
<tr>
<td>(h)</td>
<td>Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the <strong>provision of health or social care or treatment or management of health or social care systems and services</strong> on the basis of Union or Member State law or a contract with a health professional.</td>
</tr>
<tr>
<td>(i)</td>
<td>Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring <strong>high standards of healthcare</strong> and of medicinal products or medical devices.</td>
</tr>
<tr>
<td>(j)</td>
<td>Processing is necessary for <strong>archiving purposes</strong> in the public interest, or scientific and historical research purposes or <strong>statistical purposes</strong> in accordance with Article 89(1).</td>
</tr>
</tbody>
</table>