What is Confidentiality?

Within the Trust almost all staff will have access to confidential and private information. Any personal information held by the Trust is confidential. Confidential information must be used only for proper purposes, kept secure and disclosed only to those who need to know. This includes not only information in paper or electronic formats, including email, photographs, videos, audio etc., but also information that is not written down and just “known”. The information may be about staff, patients or indeed anyone whom we hold information on. The Data Protection Act 1998 and the Caldicott Principles give all individuals, patients and staff alike, the right to expect that we handle their personal information properly and to keep it confidential.

Your Responsibility

It is important therefore that you understand your responsibility in protecting any confidential information that you may use in your role, and know and understand Trust policy and your legal duty.

Anyone found to be in breach of law or Trust policy on confidentiality will be subject to the Trust’s disciplinary processes and may face dismissal or criminal prosecution.

However, the Trust supports any member of staff who, using careful consideration and professional judgement, and following the principles in this document, can satisfactorily justify any decision regarding confidentiality of information.

Using Confidential Information

You must only access and use information as part of your duties in the Trust - ask yourself “can I do my job without knowing this information?” When dealing with any kind of information remember that it is not acceptable to use Trust systems to access staff or patient information for personal uses, such as Christmas lists, birthdays, or any other use that might be taken as pure curiosity.

How to protect confidentiality - Data Protection Act 1996 and Caldicott principles

The Data Protection Act and the Caldicott Principles give individuals the right to know what information we have about them and provide a framework to ensure that personal information is handled properly. You may be granted authority to access to such information in order to undertake your duties and this information, whether clinical or non-clinical, must be treated as confidential.

Keeping Information Secure

Ensure the physical security of information, whether it is on a computer or paper record. It should never be left unattended or placed at risk (e.g. laptops are very likely to be stolen, storing confidential papers in a laptop bag, rather than separately puts them at higher risk of theft).

Before you leave a computer unattended, be sure to lock the screen (Windows Logo-L) so that no information is showing, or anyone else can access the computer.

Please check the mobile working policies if you use work-related information outside of the office or in the community.
Keeping Conversations Private

Should you need to tell another person confidential information about someone as part of your job, either over the phone or in person, then you should do this as discreetly and privately as possible. In particular, you should ensure that no-one else is able to overhear you unless if they have at least the same responsibility towards confidentiality as you.

Above all, you must never relate personal and confidential information to someone else in a public place, such as on a bus or in a café.

Electronic Information

All electronic devices must be encrypted, including laptops, CDs, DVDs and USB sticks.

No encryption password should be kept close by, or attached to, the associated encrypted media or device.

The IM&T Helpdesk can give advice on any of this.

Transferring Information

When transferring patient identifiable information it is vital that all information is sent as securely as possible. See the flowcharts at the end of this document for details about each form of communication.

Looking after Medical Records

Keeping track of patient records is vital to ensure that patient information is not mislaid. You must therefore book out, track and return records efficiently.

Whilst they are in your care, please make sure that you do not lose paper records, such as by dropping them.

What to do if data is lost

If a breach of confidentiality occurs it is important to notify your manager and reported as an information governance incident as soon as possible. All incidents will be monitored and investigated. Measures will be taken to ensure that a similar incident will not reoccur.

Speaking out

If a member of staff suspects any bad practice with regard to confidentiality then the Trust encourages them to raise the concern with their manager. All concerns must be raised in good faith and will be treated respectfully. The Trust will ensure the confidentiality of the member of staff who is making the claim.

Keeping Patients Informed

Patients must be made aware that the information they give will usually be recorded and may be shared to provide them with care and monitor quality. They should also be told that they have a choice about uses of information for activities such as education and research. If you have direct contact with patients, you must make sure that:

- You have available leaflets and other materials describing how patient information is used and that they are displayed and actively offered to patients. You should also ensure that patients understand them
- It is made clear to patients to whom and why their information is going to be disclosed
- Patients are made aware of the choices they have about the use of their information
- Any queries patients have are answered
- Patients’ rights of access, correction and choice are respected where appropriate
- Patients are made aware that information may be shared with appropriate team members in multi-agency teams
Sharing Information and Consent

Generally patient consent is always required before sharing confidential information. Ensure that where necessary you obtain written consent from patients and then store this in their medical file.

Remember that when sharing information it is important to share only what is required.

It is important to inform patients they have the right to object to the disclosure of their personal information but the patient should be made aware that this could result in health professionals not having a full picture of their needs and may affect their care. It is important for staff to strike a balance between the harm that could be done to a patient's health if information isn't used and shared, and the risk of breaching confidentiality if information is shared. If you feel sharing information is necessary to avoid or reduce harm and distress then it is likely that the legal and regulatory framework would support your decision.

Don’t forget that your duty of confidentiality extends to your staff colleagues. For example, you should not give out details such as their phone numbers or personal email addresses without their agreement.

Confidentiality and Electronic Communications

You need to be especially aware of the particular risks to confidentiality posed by new electronic communications applications. The growth of blogging and social networking websites has helped to blur the line between public and private by making it easier to share information that could result in confidentiality breaches, defamation, slander and reputational damage. The widespread use of internet enabled devices such as Smartphones, notepads, tablets and iPhones that also allow emails to be sent and received contribute to this risk. Although our Trust's policy remains that access to these sites will be blocked on the IT network, you should be aware of the consequences of sharing any work-related information outside of the Trust via electronic means.

You should avoid being included in such postings, and are reminded that posting anything which could identify a patient, or anything defamatory about the Trust, on any social networking site may lead to disciplinary action.

All staff also have a responsibility not to take photographs using their phones if it could in any way breach the confidentiality of patients, fellow staff or the Trust itself.

Similarly patients using social networking sites whilst in hospital (posting to a Facebook page, for example), should be reminded not to breach other patient or staff's confidentiality by, for example, posting photographs of the ward or of other patients.

Subject Access Requests

Under the Data Protection Act all patients and staff are allowed access to the records that the Trust holds on them by applying for a Subject Access Request. All access to health records requests are facilitated through Medical Records. All requests for information must be received in writing and have appropriate patient consent unless other legal requirements apply.

<table>
<thead>
<tr>
<th>RELATED DOCUMENTS</th>
<th>Patient Information: Principles, Guidelines and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Staff Code of Conduct</td>
</tr>
<tr>
<td></td>
<td>NHS Code of Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Health Records Procedures</td>
</tr>
<tr>
<td></td>
<td>Information Governance Policy</td>
</tr>
<tr>
<td></td>
<td>Speaking Out Policy</td>
</tr>
<tr>
<td></td>
<td>What we do with your personal information leaflet</td>
</tr>
<tr>
<td></td>
<td>Policy for the Management of Incidents</td>
</tr>
<tr>
<td></td>
<td>Serious Untoward Incident Reporting Policy</td>
</tr>
<tr>
<td></td>
<td>Social Media Policy</td>
</tr>
<tr>
<td></td>
<td>Disciplinary Policy</td>
</tr>
</tbody>
</table>

| QUERIES | Contact the Trust Secretariat or the Trust Caldicott Guardian for queries relating to confidentiality of information |
## Guidance for Sending Personal Information

### Incoming Phone Call
- Confirm the name, job title and organisation (where appropriate) to which the person requesting the information belongs
- Ask for a reason for the information and check that the request is appropriate
- Take a contact telephone number; for an organisation this should be a switchboard number only and not a mobile or personal number
- Check whether the information can be provided. If in doubt tell the enquirer you will call them back.
- Provide the information only to the person who requested it
- Ensure that you record your name, date & time of disclosure, your reason and who authorised the disclosure. Also record the information of the recipient’s name, job title, organisation & phone number where appropriate

### Outgoing Phone Call
- Do not make confidential calls where you can be overheard
- If both a landline and a mobile number are given, then use the mobile number if possible
- Check that it is the correct person that you are speaking to. If not, ask if the person can come to the phone.
- If the person cannot come to the phone, ask whom you are speaking to and check whether that person has authority to talk on behalf of the patient
- Do not leave an answerphone message unless the matter is urgent and you can’t try calling again.
- If you have to leave a message, either with another person or on an answerphone, give only the barest of details so that confidentiality is maintained
- Enter details of the conversation on the appropriate record

### Fax
- Only fax confidential information if absolutely necessary.
- Always try to send to a safe haven, (where the fax is in a secure office)
- Personal details should be faxed separately from clinical details – remember to include the NHS number
- Telephone ahead to check the fax number & inform the recipient that you are going to fax confidential information.
- Ask them to acknowledge the receipt of the fax
- Always double check the fax number and be careful to dial it correctly.
- Ensure you have a fax cover sheet which marks who the fax is for and make sure to write “Private & Confidential” on it.
- If appropriate request a report sheet to check that the fax transmission was successful
- Do not leave information on the fax machine

### Telephone
- If both a landline and a mobile number are given, then use the mobile number if possible
- Check that it is the correct person that you are speaking to. If not, ask if the person can come to the phone.
- If the person cannot come to the phone, ask whom you are speaking to and check whether that person has authority to talk on behalf of the patient
- Do not leave an answerphone message unless the matter is urgent and you can’t try calling again.
- If you have to leave a message, either with another person or on an answerphone, give only the barest of details so that confidentiality is maintained
- Enter details of the conversation on the appropriate record
## Guidance for Sending Personal Information

### Outgoing Post
- Confirm the name, department and address of the recipient. Double check if in doubt.
- Confirm that the reason for the information request is appropriate.
- If it contains confidential information, mark the envelope “private and confidential”.
- If you want the recipient to open it, mark it “addressee only”.
- Use tamper-proof packaging and seal the envelope robustly and securely.
- When appropriate the post must be sent by tracked post, sending mail by Special Delivery is the most secure way of sending post as it is tracked at every stage.
- Where necessary, ask the recipient to confirm receipt of the post.

### Transportation
- Person identifiable information should only be taken off site when absolutely necessary.
- Record what information you are taking off site and why, and if applicable where and to whom you are taking it.
- Information must be transported in a sealed container.
- Never leave person identifiable information unattended.
- Ensure that information is returned back to its site as soon as possible.
- Record that the information has been returned.

### Email
- REMEMBER: Your emails may be disclosed to the public. Always be professional.
- Only send confidential data over email if absolutely necessary. Always check you have entered the correct email address.
- If you need to send patient identifiable information make sure you do it by encrypted email (see IG06: How to Encrypt Emails).
- The email will only be secure if you send it to a member of staff within the Trust or if you are sending it via NHS mail accounts.
- If you have to send Word documents or Excel spreadsheets, make sure they are password protected. Send the password in a separate email.
- Check that you haven’t selected “reply all” by mistake.
- Ensure that anyone cc’d or bc’d actually needs to receive the confidential information.
- Where applicable, tick the “Delivery Receipt” and/or “Read Receipt” boxes prior to sending.