

# COMMISSIONING PCT CODE OF CONDUCT FOR EMPLOYEES IN RESPECT OF CONFIDENTIALITY 2010 - 2012

## **Approval Process**

Lead Author: Malcolm Finney  
Clinical Information Manager

Reviewed by: Information Governance Steering Group

Approved by: Information Governance Steering Group

Ratified by: Healthcare Governance Committee

Date ratified: May 2010

Version: 2.3

Review date: May 2012  
(or earlier if significant change to local or national requirements)

Valid on: May 2010

## Code of Conduct for Employees in Respect of Confidentiality

### Document Control Sheet

Development and Consultation:	Policy developed in consultation with the Information Governance Steering Group and endorsed by the Healthcare Governance Committee and PCT Board.
Dissemination	This policy will be disseminated to the Human Resources team for inclusion in induction papers and all services within the PCT made aware.
Implementation	The Medical Director is responsible for monitoring the application of the policy by ensuring that:- <ul style="list-style-type: none"> <li>• The policy is brought to the attention of all employees and building users</li> <li>• Managers are aware of their responsibilities for ensuring that staff under their control implement the policy</li> <li>• Staff are informed and consulted as appropriate</li> <li>• Appropriate training and guidance is provided to staff</li> <li>• Corporate business processes support the implementation of the policy.</li> </ul>
Training	Training will be undertaken as part of the PCT's ongoing processes.
Audit	Implementation of the Policy will be monitored on a regular basis.
Review	This policy will be reviewed two yearly, or earlier if there are changes in procedures or legislation.
Links with World Class Commissioning	This policy supports the PCT in its compliance with World Class Commissioning Competency 4 and 8
Links with other DtGP	The Policy should be read in conjunction with: <ul style="list-style-type: none"> <li>NHS Code of Confidentiality</li> <li>NHSC E-mail Acceptable Use Policy</li> <li>NHSC Safe Haven Policy</li> <li>NHSC Removable Media Policy</li> <li>NHSC Destruction and Disposal Policy</li> </ul>
Equality and Diversity	The Governance team carried out a Rapid Equality & Diversity Impact assessment and concluded the policy is compliant with the PCT Equality and Diversity Policy. No negative impacts were found.

### Revisions

Version	Page/ Para No	Description of change	Date approved
1		Discussed by Information Governance Steering Group	
2		For endorsement by IG Steering Grp pre approval by Healthcare Governance Committee	
2.1	Whole document	Final formatting and changes pre dissemination	March 2008
2.2	Whole document	Full review before requesting endorsement as a working draft by IG Steering Group and ratification by Healthcare Governance Committee. Further amendments anticipated once Homeworking Policy finalised and ratified	April 2010

Code of Conduct for Employees in Respect of Confidentiality

Version	Page/ Para No	Description of change	Date approved
2.3	Whole document	by Board. Throughout document reviewed use of phrase 'service users' as requested by Healthcare Governance Committee Original Appendix 4 removed after discussion and agreement with HR and alternative Appendix 4 substituted.	May 2010

## **CODE OF CONDUCT FOR EMPLOYEES IN RESPECT OF CONFIDENTIALITY**

**Please note that this document should be read and understood prior to the contract of employment or other confidentiality agreement being signed. If there is anything that is not clear please contact your manager.**

### **1. Purpose of the Code**

- 1.1 This policy details required practice for those who work within or under contract to the Trust concerning maintaining confidentiality for all personally identifiable information. For the purposes of this document the term “employee” is used as a convenience to refer to all those to whom this code should apply. Whilst directed at Trust staff it is also relevant to any one working in and around the Trust to include contractors, agency staff, students and volunteers.
- 1.2 All employees working in the NHS are bound by a statutory duty of confidence to protect personal information. This is a requirement established within Common Law, the Data Protection Act 1998, Article 8 of the Human Rights Act 1998 and the Code of Practice on Confidentiality published in November 2003. In addition, for clinical and other professional staff it is contained within their own professional Code/s of Conduct. (Appendix 2)
- 1.3 This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. It should be noted that employees (e.g. Complex Case and Exceptional Case Teams) also come into contact with non-person identifiable information which should be also be treated with the same degree of care e.g. business in confidence information such as patient referral letters, discharge summaries, waiting list data, consultants work loads, clinic lists, Practice Based Commissioning Business Cases, staff records, Patient Advice and Liaison Service, Choice and Book
- 1.4 The principle behind this Code of Practice (Code) is that no employee shall knowingly breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trusts security systems or controls in order to do so.
- 1.5 This Code has been written to meet the requirements of:
  - The Data Protection Act 1998
  - The Human Rights Act 1998
  - The Computer Misuse Act 1990
  - The Copyright Designs and Patents Act
- 1.6 This Code has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. Breach of confidentiality of information gained, either directly or indirectly in the course of duty is a disciplinary offence that could result in dismissal. (See Appendix 3)

## 2. Definitions

See also Glossary of Terms – Appendix 1

### 2.1 Confidentiality of Information

All employees are responsible for maintaining the confidentiality of information.

### 2.2 Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored.

For example, information may be held on paper, floppy disc, CD, computer file or printout, video, photograph or even heard by word of mouth.

It includes information stored on portable devices such as laptops, palmtops, mobile phones and digital cameras.

It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes any company e.g. PCT business confidential information.

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) can be sufficient to identify an individual.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

During your duty of work you should consider all information to be sensitive, even something as simple as a patient's name and address. The same standards should be applied to all information you come into contact with.

### 2.3 Ensuring that the data subject understands what use will be made of their information

Staff and data subjects (or their representatives) must understand how we will use information about them. Achieving this understanding will therefore depend on staff giving the data subject relevant information about the purposes of processing information about them and any likely disclosures. A Confidentiality Statement should be completed with the data subject/service user and they should be asked to sign to confirm their understanding and agreement. The practitioner responsible for the care of the service user *must* discuss the uses of their information with them. Leaflets are useful for reinforcing information given to

## Code of Conduct for Employees in Respect of Confidentiality

a person, but are not in themselves sufficient. Any explanation should include as a minimum:

- That the main use of the information will be to manage the data subject's care and treatment, and that it is very important that we have full and accurate information if we are to provide the best care.
- That we also use their information to check the quality of the care that they and other service users receive, to ensure that this is of the right standard. This process is called audit. Everyone involved in audit has to follow the same strict rules on confidentiality.
- That you work as part of a team and will share information about the data subject/service user with the team if it is necessary to provide the best care for them. Explain who is a member of your team. If you work with members of another agency then you should explain that information may be passed to that agency if it is necessary to provide their care, but that the agency has also signed up to the same standards of confidentiality.
- That they have a right of access to their health records which can be explained on request.
- That we send anonymous information to the Department of Health to allow us to manage services and monitor effectiveness.

It may also be appropriate or necessary to discuss the use of the subject's information at other times during their care, for example:

- When transferring their care to someone or somewhere else.
- When their legal status changes (for example, the section of the Mental Health Act which applies to them, or if they are diagnosed with a notifiable disease).

### 2.4 Ensuring that the data subject gives their consent for such use.

The data subject must consent to our proposed uses of their personal information. They therefore need sufficient information about the potential uses of their information to make an informed choice. It is not usual practice to obtain written consent to the use of information for care and treatment, although this is required for some other uses (such as research). Seek advice from the Trust's Caldicott Guardian if in doubt.

#### *What if patients do not consent?*

If service users do not consent to our proposed use of their information then we cannot use it in that way. It is important that the data subject/service users fully understand the implications of such a decision and in serious situations where the well-being of the data subject or others may be compromised you should seek advice from the Trust's Caldicott Guardian, and the senior practitioner

## Code of Conduct for Employees in Respect of Confidentiality

responsible for the service user. Such a decision must be carefully documented and reported to the responsible practitioner.

### 2.5 Ensuring that the data subject understands the limits of confidentiality

You should explain to the subject that in some circumstances you will be obliged to pass on or act upon information even if they object. This will apply if a failure to pass on information may lead to harm to the service user or someone else. There are also certain legal requirements to pass on information that can be explained to the patient if required.

### 2.6 Collecting only what is necessary

You should only collect as much personal information as is necessary for the agreed purpose, and no more. The information collected must be adequate but not excessive. Clearly most healthcare records are by necessity very detailed, but they must nevertheless be accurate and relevant. Where information is extracted for other agreed purposes (for example audit) there should be a sound rationale for every piece of information that is used. Personal identifiers should be removed from the data if they are not strictly necessary for the intended use.

### 2.7 Recording the information accurately

You have a legal obligation to ensure that any personal information you are holding is accurate. Data is regarded as inaccurate if it is incorrect or misleading as to any matter of fact. Data subjects have a legal right to have factual inaccuracies corrected or removed from records, and to have an entry made in their record if they disagree with a statement of opinion.

## 3. Requests for Information on Data Subjects/Service Users and Staff

- Never give out information on data subjects/service users or staff to persons who do not “need to know” in order to provide health care and treatment.
- All requests for person identifiable information should be based on a justified need and in some cases may also need to be authorised by the PCT Caldicott Guardian (for health care information – Dr Christine MacLeod, Medical Director).

If you have any concerns about disclosing/sharing person identifiable information you must discuss with your manager and if they are not available, someone with the same or similar responsibilities. If you cannot find anyone to discuss the issue with, you should wait until someone is available and only disclose when you have discussed with a manager.

### 3.1 Telephone Enquiries

If a request for information is made by telephone,

- Always check the identity of the caller and

## Code of Conduct for Employees in Respect of Confidentiality

- Check whether they are entitled to the information they request.
- Take a number, verify it independently and call back if necessary.

Remember that even the fact that a patient is in hospital, is a user of the service you work within, or is a member of staff, this is confidential. If in doubt consult your manager.

### 3.2 Requests for Information by the Police and media

With respect to the Police

- Requests for information from the Police should always be referred to the Caldicott Guardian or the Information Governance Manager.

With respect to the Media

- Do not give out any information under any circumstances. Only Senior Managers are authorised to do so. If you receive any request from the media by personal visit or by phone refer the person to the Director or Assistant Director of Communications.

### 3.3 Disclosure of Information to Other Employees of the PCT

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

- Always check the member of staff is who they say they are.
- This can be achieved by checking the employee's ID badge and/or their internal extension number or bleep number prior to giving them any information.
- If possible also check whether they are entitled to the information.
- Don't be bullied into giving out information.

If in doubt, check with the person in charge of the data subjects care or your manager.

### 3.4 Abuse of Privilege

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

If you have concerns about this issue please discuss with your line manager.

### 3.5 Carelessness

- Do not talk about patients/service users in public places or where you can be overheard.
- Do not leave any medical records or confidential information lying around unattended.

## Code of Conduct for Employees in Respect of Confidentiality

- Make sure that any computer screens, or other displays of information, cannot be seen by the general public.
- Always lock your computer screen if you leave it unattended – by pressing the Ctrl/Alt/Delete keys together and then choosing the 'Lock' option.

### 4. Transfer of Information (see also Safe Haven Policy)

#### 4.1 Use of Internal and External Post

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

**Internal** mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate.

**External** Mail must also observe these rules. Special care should be taken with person identifiable information sent in quantity, such as case notes, or collections of patient records on paper, floppy disc or other media. These should be sent by Recorded Delivery or by NHS courier, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

**Electronic and removable media** should be encrypted/password protected. Advice on how to password protect files is available from (IT Helpdesk 0800 996 996). [See also Removable Media Policy](#)

**Case notes** and other bulky material should only be transported in the approved boxes and never in dustbin sacks, carrier bags or other containers. These containers should not be left unattended unless stored, waiting for collection, in a secure area e.g. ideally locked. The containers should only be taken and transported by the approved carrier.

**Blood samples** etc. should also only be transported within the correct authorised containers and should not be left lying around within the GP practice or when they have been delivered to the laboratory.

#### 4.2 Faxing

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

- Use a cover sheet that indicates confirmation of receipt is required.

#### 4.3 Email

##### [See Email Acceptable Use policy](#)

Please seek advice from your manager if you have the need, or possible need, to e-mail person identifiable information.

The e-mail transmission of this information internally over the PCT network can pose serious risks to confidentiality, and should always be avoided unless essential to the delivery of health care. In this case strict principles should always be followed.

**Personal identifiers should be removed** wherever possible, and only the minimum necessary information sent, this may be considered to be the NHS number but no name or address. This in itself can pose problems as the wrong number may be typed.

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

**External** transfers should only take place to persons with access to a secure account compatible with nhs.net. In exceptional cases it may be necessary to e-mail person identifiable information or sensitive or confidential information to persons who only have Internet access. In such cases the potential risk of loss and the insecure nature of using the Internet should be explained and communicated to the intended recipient and their agreement recorded.

#### 5. Storage of Confidential Information

Paper-based confidential information should always be kept locked away and preferably in a room that is locked, and in some cases alarmed (e.g. GUM records are sensitive) when unattended, particularly at nights and weekends or when the building/office will be un-occupied for a long period of time.

PC-based information should not be saved onto local hard drives or onto removable media, but onto the PCT's networked 'restricted' drive. Floppy discs, CDs, and other media should be kept in locked storage.

#### 6. Disposal of Confidential Information

##### [See Destruction and Disposal Policy](#)

When disposing of **paper-based person-identifiable information** or confidential information always use 'Confidential Waste' bins/sacks/shredders. Do not store confidential information where it could be confused with general waste.

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

**Floppy discs/CDs** containing confidential information must be either reformatted or destroyed. Computer files with confidential information no longer required must be deleted from both the PC and the server if necessary.

**Computer hard disks** are disposed of by the ASP IT department.

**X-rays** that are no longer required must be disposed of in the correct manner and guidelines are available which detail the companies who will provide secure destruction of the x-rays. These must not be disposed of in any waste bins, other confidential waste disposal method e.g. sacks, shredders, or in clinical waste sacks. The disposal and destruction of x-rays can cause a threat to the health of anyone trying to destroy them unless the correct method is used – and this is only available by specialist suppliers.

## 7. Confidentiality of Passwords

Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone.

- Passwords should not be written down.
- Passwords should not relate to the employee or the system being accessed.

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

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to the Information Governance Manager and may result in a disciplinary action and also to a breach of the Computer Misuse Act 1990 and/or the Data Protection Act 1998, which could lead to criminal action being taken against you.

## 8. Working at home

### Home working Policy under development

It is sometimes necessary for employees to work at home. If you need to do this you would first need to gain approval from your manager. If they agree you would need to ensure a full assessment is carried out and be aware that there is personal liability under the Data Protection Act 1998 and your contract of employment for breach of certain requirements:

It is particularly important that paper copies of information containing person identifiable information are logged in and out (if there is a legitimate need to be taken off site).

## Code of Conduct for Employees in Respect of Confidentiality

- Ensure any personal information in manual form e.g. patient/staff files, or electronic format e.g. floppy discs/CDs, are in sealed containers prior to them being taken out of the PCT building/s.
- Make sure they are locked and out of sight in the boot of the car or carried on your person while being transported from your work place to your home.

While at home you have personal responsibility to ensure the records are kept secure and confidential. This means that other members of your family and/or your friends/colleagues must not be able to see the content or outside folder of the records.

- You must not let anyone have any access to the records.
- Other family members must not be able to access this information.

When returning information to your work place you must ensure that the log is updated to reflect this.

### **9. Copying of software**

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

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

### **10. General Provisions**

#### **10.1 Interpretation**

If any person requires an explanation concerning the interpretation or the relevance of this code of conduct, they should discuss the matter with their line manager, a member of the Information Governance team or the Caldicott Guardian.

The Caldicott Guardian is Dr Christine MacLeod, Medical Director

As a consequence of your employment by Cambridgeshire Primary Care Trust, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of the Trust. This condition applies during your relationship with the Trust and after the relationship ceases.

#### **10.2 Non-Compliance**

Non-compliance with this code of conduct by any person working for the PCT may result in disciplinary action being taken in accordance with the PCT'S disciplinary procedure, and may lead to dismissal for gross misconduct.

## Code of Conduct for Employees in Respect of Confidentiality

To obtain a copy of the disciplinary procedures please discuss with your manager or the Human Resources department.

### 10.3 Amendments

This code will be amended as necessary to reflect the PCT's development of policies and procedures and the changing needs of the NHS.

## 11. Confidentiality Statement

All PCT faxes and e-mails should contain the disclaimer as detailed below.

*This message may contain confidential and privileged information. If you are not the intended recipient please accept our apologies. Please do not disclose, copy, or distribute information in this e-mail or take any action in reliance on its contents. To do so is strictly prohibited and may be unlawful. Please inform us that this message has gone astray before deleting it. Thank you for your co-operation.*

## 12. Sources of Reference

NHS Confidentiality Code of Practice 2003

[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_4069253](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253)

General Protocol For Protecting And Using Personal Information Within  
Cambridgeshire & Peterborough - November 2007

### 13. Appendix 1 Glossary of Terms

<b>Patient identifiable information</b>	<p>Key identifiable information includes:</p> <ul style="list-style-type: none"><li>• a person's name, address, full post code, date of birth;</li><li>• pictures, photographs, videos, audio-tapes or other images of patients;</li><li>• NHS number and local patient identifiable codes;</li><li>• anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.</li></ul>
<b>Anonymised</b>	<p>This is information which does not identify an individual directly, and information which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.</p>
<b>Pseudonymised</b>	<p>This is like anonymised information in that in the possession of the Information holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.</p>
<b>Clinical Audit</b>	<p>The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services. This should be distinguished from studies that aim to derive, scientifically confirm and publish generalisable knowledge. The first is an essential component of modern healthcare provision, whilst the latter is research and is not encompassed within the definition of clinical audit in this document.</p>
<b>Explicit or Express Consent</b>	<p>This means articulated patient agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.</p>
<b>Implied Consent</b>	<p>This means patient agreement that has been signalled by behaviour of an informed patient.</p>
<b>Disclosure</b>	<p>This is the divulging or provision of access to data.</p>

## Code of Conduct for Employees in Respect of Confidentiality

<b>Healthcare Purposes</b>	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.
<b>Information Sharing Protocols</b>	Documented rules and procedures for the disclosure and use of person identifiable information, which specifically relate to security, confidentiality and data destruction, between two or more organisations or agencies.
<b>Medical Purposes</b>	As defined in the Data Protection Act 1998, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001 explicitly broadened the definition to include social care.
<b>Public Interest</b>	Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.
<b>Social Care</b>	Social care is the support provided for vulnerable people, whether children or adults, including those with disabilities and sensory impairments. It excludes “pure” health care (hospitals) and community care (e.g. district nurses), but may include items such as respite care. There is therefore, no clear demarcation line between health and social care. Social care also covers services provided by others where these are commissioned by CSSRs (Councils with Social Service Responsibilities).

## 14. Appendix 2

### Professional codes of confidentiality

#### 1. Doctors

##### **Extract from General Medical Council “Confidentiality – Protecting and Providing Information”**

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

- inform patients about the disclosure, or check that they have already received information about it;
- anonymise data where unidentifiable data will serve the purpose;
- be satisfied that patients know about disclosures necessary to provide their care, or for local clinical audit of that care, that they can object to these disclosures but have not done so;
- seek patients’ express consent to disclosure of information, where identifiable data is needed for any purpose other than the provision of care or for clinical audit – save in the exceptional circumstances described in this booklet;
- keep disclosures to the minimum necessary; and
- keep up to date with and observe the requirements of statute and common law, including data protection legislation.

You must always be prepared to justify your decisions in accordance with this guidance

#### 2. Nurses and Midwives

##### **Extract from Nursing and Midwifery Council “The NMC Code of Professional Conduct: Standards for Conduct, Performance and Ethics”**

As a registered nurse, midwife or health visitor, you must protect confidential information

- You must treat information about patients and clients as confidential and use it only for the purposes for which it was given. As it is impractical to obtain consent every time you need to share information with others, you should ensure that patients and clients understand that some information may be made available to other members of the team involved in the delivery of care. You must guard against breaches of confidentiality by protecting information from improper disclosure at all times.
- You should seek patients’ and clients’ wishes regarding the sharing of information with their family and others. When a patient or client is considered incapable of giving permission, you should consult relevant colleagues.

## Code of Conduct for Employees in Respect of Confidentiality

- If you are required to disclose information outside the team that will have personal consequences for patients or clients, you must obtain their consent. If the patient or client withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:
  - they can be justified in the public interest (usually where disclosure is essential to protect the patient or client or someone else from the risk of significant harm)
  - they are required by law or by order of a court
- Where there is an issue of child protection, you must act at all times in accordance with national and local policies.

### 3. Social Workers

#### **Extract from British Association of Social Workers “Code of Ethics: Privacy, confidentiality and records”**

Social workers will:

- Respect service users' rights to a relationship of trust, to privacy, reliability and confidentiality and to the responsible use of information obtained from or about them;
- Observe the principle that information given for one purpose may not be used for a different purpose without the permission of the informant;
- Consult service users about their preferences in respect of the use of information relating to them;
- Divulge confidential information only with the consent of the service user or informant, except where there is clear evidence of serious risk to the service user, worker, other persons or the community, or in other circumstances judged exceptional on the basis of professional consideration and consultation, limiting any such breach of confidence to the needs of the situation at the time;
- Offer counselling as appropriate throughout the process of a service user's access to records;
- Ensure, so far as it is in their power, that records, whether manual or electronic, are stored securely, are protected from unauthorised access, and are not transferred, manually or electronically, to locations where access may not be satisfactorily controlled;
- Record information impartially and accurately, recording only relevant matters and specifying the source of information.
- The sharing of records across agencies and professions, and within a multi-purpose agency, is subject to ethical requirements in respect of privacy and confidentiality. Service users have a right of access to all information recorded about them, subject only to the preservation of other persons' rights to privacy and confidentiality.

#### **4. Health Informatics Professionals**

##### **Extract from UK Council for Health Informatics Professionals “Code of Conduct: Protecting and acting in the interests of patients and the public”**

All health informatics professionals shall, to the best of their ability, protect and promote the interests of patients and the public by:

- Ensuring that information systems and equipment for which they are responsible are procured, installed, maintained and operated professionally, efficiently and safely, and provide good value for the public money invested in them;
- Ensuring the security, confidentiality, accuracy and integrity of information, and protecting the safety of patients and the public, both directly through their personal actions and indirectly through the design and operation of any information systems for which they are responsible;
- Reporting to the proper authorities any improper or misleading use of information, whether accidental or deliberate, or misconduct by any person in connection with the procurement, operation or use of information systems and equipment;
- Promoting the appropriate use of information to enhance patient and public involvement and to support patient empowerment, dignity and choice.

## RELEVANT ACTS OF PARLIAMENT AND NHS GUIDELINES AND WHAT THEY MEAN FOR EMPLOYEES

<b>Requirement</b>	<b>What it covers</b>	<b>Personal responsibilities</b>	<b>Penalties for breaches</b>
Data Protection Act 1998	Person identifiable information about living individuals – manual and automated records (e.g. on computer, video tape, digital images)	Keep all person identifiable information secure and confidential – see Code of Conduct for specific details	Unauthorised disclosure of personal identifiable information could lead to court action and a criminal conviction and/or the payment of compensation to a claimant
Human Rights Act 1998 (Article 8)	An individual's right to privacy for themselves and their family members	As above	As above
Computer Misuse Act 1990	Unauthorised access to computer held programs and information/data	Do not use any other persons access rights (e.g. user id and password) to access a computer database	A criminal record and a prison sentence of up to 5 years
Common Law of Confidentiality	An individual's right to confidentiality of their information when alive and once they have died	Keep all information secure and confidential. Also remember this covers wishes of deceased persons – if it is recorded that they do not want details of their treatment disclosed when they die this wish will normally need to be respected	Disciplinary action and possible dismissal
Caldicott	Security and confidentiality of personal health and social care information for patients and service users	See Code of Conduct – further information available from Trust/Practice Caldicott Guardian or Information Governance Manager	Disciplinary action and possible dismissal
Contract of Employment	Employees responsibilities including security and confidentiality of any information accessed during the course of work	Comply with contract and Code of Conduct	Disciplinary action and possible dismissal