Data Protection and Code of Confidentiality Policy

<table>
<thead>
<tr>
<th>REFERENCE NUMBER</th>
<th>IG 05 / 0v4 February 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION</td>
<td>V1.0</td>
</tr>
<tr>
<td>APPROVING COMMITTEE &amp; DATE</td>
<td>Clinical Executive Committee 12.2.13</td>
</tr>
<tr>
<td>REVIEW DUE DATE</td>
<td>February 2016</td>
</tr>
</tbody>
</table>
West Lancashire CCG is committed to ensuring that, as far as it is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on the basis of their age, disability, gender, race, religion/belief or sexual orientation.

Should a member of staff or any other person require access to this policy in another language or format (such as Braille or large print) they can do so by contacting the West Lancashire CCG who will do its utmost to support and develop equitable access to all policies.

Senior managers within the CCG have a responsibility for ensuring that a system is in place for their area of responsibility that keeps staff up to date with new policy changes.

It is the responsibility of all staff employed directly or indirectly by the CCG to make themselves aware of the policies and procedures of that CCG.
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PURPOSE</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>SCOPE</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>GUIDANCE</td>
<td>3</td>
</tr>
<tr>
<td>3.1</td>
<td>Duties and responsibilities</td>
<td>3</td>
</tr>
<tr>
<td>3.1.1</td>
<td>NHS West Lancashire CCG Governing Body</td>
<td>3</td>
</tr>
<tr>
<td>3.1.2</td>
<td>Chief Officer</td>
<td>4</td>
</tr>
<tr>
<td>3.1.3</td>
<td>Caldicott Guardian</td>
<td>4</td>
</tr>
<tr>
<td>3.1.4</td>
<td>All Managers</td>
<td>4</td>
</tr>
<tr>
<td>3.1.5</td>
<td>Information Governance Lead for CCG</td>
<td>4</td>
</tr>
<tr>
<td>3.1.6</td>
<td>Subject Access- Local Lead</td>
<td>5</td>
</tr>
<tr>
<td>3.1.7</td>
<td>All Staff</td>
<td>5</td>
</tr>
<tr>
<td>3.2</td>
<td>Use and Disclosure of Personal Information</td>
<td>5</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Information Quality</td>
<td>5</td>
</tr>
<tr>
<td>3.3</td>
<td>Informing people about use of their information</td>
<td>6</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Providing advice and responding to individuals</td>
<td>6</td>
</tr>
<tr>
<td>3.4</td>
<td>Access to Records</td>
<td>6</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Access to Records</td>
<td>6</td>
</tr>
<tr>
<td>3.5</td>
<td>Staff training and awareness</td>
<td>7</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Training</td>
<td>7</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Induction</td>
<td>7</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Contracts of Employment</td>
<td>7</td>
</tr>
<tr>
<td>3.5.4</td>
<td>Disciplinary</td>
<td>7</td>
</tr>
<tr>
<td>3.6</td>
<td>Confidentiality and Caldicott Principles</td>
<td>7</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Confidentiality</td>
<td>7</td>
</tr>
<tr>
<td>3.6.2</td>
<td>Confidentiality and research</td>
<td>7</td>
</tr>
<tr>
<td>3.6.3</td>
<td>Data Protection and confidentiality audits</td>
<td>7</td>
</tr>
<tr>
<td>3.6.4</td>
<td>Information Governance Toolkit and annual performance</td>
<td>8</td>
</tr>
<tr>
<td>3.7</td>
<td>Records Management</td>
<td>8</td>
</tr>
<tr>
<td>3.8</td>
<td>Security and Confidentiality</td>
<td>8</td>
</tr>
<tr>
<td>3.9</td>
<td>Monitoring of Compliance</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>REFERENCES AND BIBLIOGRAPHY</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>ASSOCIATED DOCUMENTS</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>APPENDICES</td>
<td>10</td>
</tr>
<tr>
<td>Appendix 1</td>
<td>The Data Protection Act 1998 Principles</td>
<td>10</td>
</tr>
<tr>
<td>Appendix 2</td>
<td>Exemptions to the Data Protection Act 1998</td>
<td>13</td>
</tr>
<tr>
<td>Appendix 3</td>
<td>Caldicott principles for handling patient-identifiable information</td>
<td>14</td>
</tr>
<tr>
<td>Appendix 4</td>
<td>General Guidance</td>
<td>15</td>
</tr>
<tr>
<td>Appendix 5</td>
<td>Glossary of Terms/legislations and guidance</td>
<td>19</td>
</tr>
</tbody>
</table>
1. PURPOSE

The Data Protection Policy sets out how the organisation will meet its obligations to comply with confidentiality and information security standards. The organisation must ensure that measures are in place to meet the legislation set out in the Data Protection Act 1998.

The CCG has an obligation to comply with all appropriate legislation in respect of data, information and information technology. Appropriate legislation is shown at section 4 and appendix 5 of this policy.

The CCG needs to collect and use certain types of information about people as part of core business activities. This includes ‘personal data’ as defined by the Data Protection Act 1998.

The CCG will meet its obligations to comply with the Data Protection Act and other guidance and standards of confidentiality and information security by:

- ensuring that all members of staff are aware of, understand and fully comply with the Data Protection Act 1998
- ensuring that all members of staff, with responsibility for processing patient-identifiable information, are aware of and comply with the Caldicott principles
- ensuring that all members of staff are aware of the Department of Health publication, Confidentiality: NHS Code of Practice, 2003 which describes an agreed set of guidelines and has the endorsement of the Information Commissioner, the BMA and the GMC setting out individual and organisational responsibilities covering both confidentiality and the Data Protection Act 1998.
- Ensuring that the CCG has procedures in place to mitigate information security breaches, can demonstrate assurance regarding business continuity, and comply with records management requirements.

2. SCOPE

This policy applies to staff employed by or working on behalf of NHS West Lancashire Clinical Commissioning Group (CCG) including contracted, non-contracted, temporary, honorary, secondments, bank, agency, students, volunteers or locums.

3. GUIDANCE

3.1. Duties and Responsibilities

3.1.1. NHS West Lancashire CCG Governing Body

It is the role of the NHS West Lancashire CCG Governing Body to define the CCG’s policy in respect of information governance, taking into account the legal
and NHS requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

3.1.2. Chief Officer

The Chief Officer, as Accountable Officer of NHS West Lancashire CCG, is the Data Controller and has overall accountability and responsibility for ensuring compliance with the NHS West Lancashire CCG Data Protection Policy.

The Chief Officer has a duty to ensure that:

- staff are aware of the need to comply with the Data Protection Act, 1998
- staff are aware of the requirements of the common law Duty of Confidence as set out in the NHS Code of Confidentiality
- arrangements with third parties who process personal data on behalf of the organisation are subject to a written contract which stipulates appropriate compliance with security and confidentiality requirements.

3.1.3. Caldicott Guardian

The Caldicott Guardian for NHS West Lancashire CCG is responsible for:

- ensuring that the organisation’s processes satisfy the highest practical standards for handling patient information. The safe recording, storing and retention of all personal data and ensuring all information flows are mapped to exclude any leaks of information
- agreeing and reviewing protocols for governing the transfer and disclosure of patient-identifiable information across the organisation, its partner organisations, supporting agencies and third parties
- ensuring appropriate information sharing agreements are in place where information is shared with third parties
- any breaches of confidentiality or security are investigated

3.1.4. All Managers

All managers are responsible for ensuring that:

- Staff are aware of this policy
- This policy, and any subsequent supporting staff guidance, is built into local processes and that there is on-going policy compliance/adherence on a day to day basis
- Any breaches, or suspected breaches of confidentiality, or incidences of non-compliance with the principles of the Data Protection Act 1998, must be reported in line with the organisation’s incident reporting procedures.

3.1.5. Information Governance Lead for the CCG

The information governance lead for the CCG will be supported by the Head of Information Governance (based in CSU) to ensure that Data Protection and Caldicott principles are fully observed. Specifically, they are responsible for:
ensuring that standards and procedures are documented and actively implemented in every location where information is collected and used
ensuring that staff are properly trained and equipped to fulfil their responsibilities
making available adequate resources for reviewing, monitoring and continually improving security and data quality
ensuring compliance with any requirements of the Information Commissioner’s Office including annual notification
advising and updating the organisation’s policies in relation to directives/guidance from the Information Commissioner, Department of Health and new information about the information governance toolkit
raising awareness of data protection issues on a constant basis to CCG staff providing guidance on data protection issues to all staff and developing and maintaining related policies, protocols, strategies and procedures
liaison with the organisation’s lead for Subject Access Requests under the Data Protection Act 1998.
ensuring that data protection and confidentiality audits are carried out
investigating data protection/confidentiality breaches

3.1.6. Subject Access – Local Lead CCG

A local lead CCG responsible for responding to Subject Access requests, will be identified to ensure the requirements of the Subject Access Policy are implemented.

3.1.7. All Staff

All staff must meet the standards described in the Department of Health publication Confidentiality: NHS Code of Practice, 2003, which is a guide to the required practice for those who work within or under contract to the NHS.

All staff members must sign and comply with the CCG’s annual Information Governance Confidentiality Code of Conduct Policy

Additionally, health and other professionals working in the NHS are bound by their own professional code(s) of conduct in respect of confidentiality.

Confidentiality and compliance with the Data Protection Act is set out in NHS contracts of employment as a specific requirement linked to disciplinary procedures. All staff will sign a confidentiality undertaking as part of their contract of employment before accessing the organisation’s computer systems.

All breaches of confidentiality and information security, whether accidental or deliberate, will be investigated by the CCG, and if deemed to be a serious offence, this may result in disciplinary action.

3.2. Use and Disclosure of Personal Information

3.2.1. Information Quality
Personal data held on any media must be accurate and up to date. The CCG will ensure data quality assurance checking is undertaken.

3.3. Informing people about the use of their information

The Data Protection Act 1998 states that individuals have to be provided with information where organisations or person(s) hold and use their personal information, the organisation will provide information as required:

- The purposes for which it is being used
- The likely disclosures of their information
- The likely consequences of the processing
- Any other information that is necessary

3.3.1. Providing advice and responding to individuals about the use of their information

The organisation will inform individuals if their information is to be used for another purpose or disclosed to a person or organisation that the individuals would not have anticipated.

The Data Protection Act gives the 'subject' the right to contact the organisation about a number of issues relating to use of their personal information, this may include:

- Objections to how their personal information is processed
- Requests for certain possible disclosures of their information to be restricted
- Requests for detailed information about how their information is used by the organisation

Advice must be sought from the Caldicott Guardian and/or the Information Governance Team at the CSU to ensure satisfactory responses and actions are taken.

Significant proposed changes in the use of personal information may require the completion of a Privacy Impact Assessment (PIA).

3.4. Access to Records

3.4.1. Access to Records

The CCG will comply with the processing of requests made by data subjects, or other authorised persons as set out in the Subject Access Policy.
3.5. Staff training and awareness

3.5.1. Training

The CCG will ensure that mandatory information governance training is delivered to all staff annually, and meets the requirement for the use of the Information Governance Training Tool (IGTT), set out in the Information Governance Toolkit.

3.5.2. Induction

The CCG will provide an induction programme to all new starters.

3.5.3. Contracts of Employment

All staff contracts of employment will include a data protection and specified confidentiality clauses. Agency and contract staff must also sign confidentiality clauses before commencing work in the organisation.

All staff will be made aware of their responsibilities in connection with the legislation outlined in this policy through staff’s Statement of Terms and Conditions.

3.5.4. Disciplinary

A breach of the data protection requirements could result in disciplinary action, or possibly criminal proceedings.

All incidents must be logged following the CCG’s agreed procedures.

3.6. Confidentiality and Caldicott Principles

3.6.1. Confidentiality

All staff must be aware of, and comply with, the Caldicott Principles. All staff must sign and comply with the CCG’s Annual Code of Confidentiality Policy

3.6.2. Confidentiality and research

The confidentiality due to individuals enrolled in research programmes applies as, outlined throughout this document. All research involving NHS patients, staff or resources must be assessed by a research ethics committee and must be formally approved by management.

3.6.3. Data Protection and confidentiality audits

The Information Governance Team at the CSU will ensure that audit procedures are developed to ensure compliance with data protection and confidentiality controls.
3.6.4. Information Governance Toolkit and annual performance

An annual assessment of the CCG’s performance in relation to data protection compliance will be undertaken through the requirements of the Information Governance Toolkit.

3.7. Records Management

The CCG will review and maintain policies and procedures to ensure that the arrangements for records management meet all the legal and business requirements, from the creation to the destruction of a record.

The CCG should maintain an up to date records management policy which includes the Retention and Disposal Schedule for all records and documents in accordance with Department of Health guidelines.

3.8. Security and Confidentiality

All information relating to identifiable individuals must be kept secure at all times. The CCG will ensure that there are adequate procedures in place to protect against unauthorised access to, and processing of, information and against accidental loss, destruction and damage to this information. The NHS West Lancashire CCG Information Security Policy must be sought for guidance and compliance.

The CCG will maintain related policies on the transfer and storage of personal information and the use of electronic and mobile media.

Personal information, whether relating to patients or staff, must not be held in the personal user or shared areas of the computer network for longer than necessary and only held if the purpose can be justified.

All staff responsible for producing reports using patient identifiable information must have the length for retention of data and deletion included in the office procedures. Paper copies of reports produced for reporting purposes must be shredded or placed in the confidential waste sacks provided to await secure, confidential disposal.

3.9. Monitoring of compliance

Incidents must be reported in accordance with the CCG’s procedures.

A report of information governance related incidents will be provided to the Clinical Executive Committee on a bi-monthly basis for monitoring and appropriate action.

4.0 REFERENCES AND BIBLIOGRAPHY

The Data Protection Act 1998
5.0 ASSOCIATED DOCUMENTS

<table>
<thead>
<tr>
<th>Document</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance Policy</td>
<td></td>
</tr>
<tr>
<td>Information Security Policy</td>
<td></td>
</tr>
<tr>
<td>Subject Access Policy</td>
<td></td>
</tr>
<tr>
<td>Records Management Policy</td>
<td></td>
</tr>
</tbody>
</table>
6.0 APPENDICES

Appendix 1

THE DATA PROTECTION ACT 1998 PRINCIPLES

Objective: To ensure compliance with the Data Protection Act, 1998

The Data Protection Act 1998 regulates the processing of information about living individuals including the obtaining, use and disclosure of information and sets out the rights and responsibilities of data subjects and data users. It covers all paper and computer records.

The Data Protection Act states that anyone who processes personal data must comply with 8 principles contained in Section 1 of the Act. (Processing means anything that is done with personal information – including, but not limited to, collecting, storing, sharing and destroying it). These are normally referred to as the ‘Data Protection Principles’. The following summary sets out the implications for all staff.

Principle 1: Personal data shall be processed fairly and lawfully

The aim of this principle is to ensure that personal data are processed fairly and lawfully and in accordance with a relevant condition from the schedules of the Act. Although the Act does not state that explicit consent is required for the processing of health information, compliance with the ‘lawful’ requirement means that the common law duty of confidence must be taken into account. This duty requires that information given in confidence must not be disclosed without the consent of the giver of that information.

Compliance will be achieved by implementing the following measures:

- All staff will have a confidentiality clause in their contract of employment.
- An approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information.
- All users of records, IM&T equipment and systems are required to sign a written confidentiality agreement. The Information Governance Code of Confidentiality Policy covers this. This undertaking will form part of the contract of employment with the member of staff. The conditions in the agreement must be clearly explained.
- Third party contractors working for the organisation are required to sign a confidentiality agreement before they are connected to the organisation’s IM&T facilities.
- Informing patients/service users how their data will be processed. This means fully describing how the data will be used and for what purposes. The organisation will produce and maintain patient information leaflets describing how the information will be protected and the purposes for which healthcare information is used. These leaflets will be clearly displayed for persons to read or take away with them.
• Ensuring that the conditions in Schedules 2 and 3 of the Data Protection Act 1998 are met. Schedule 2 describes conditions that must be met in the case of all processing of personal data (except where a relevant exemption applies). Schedule 3 provides a list of conditions that must be met in the case of sensitive data. The details of this are set out in Appendix 2.

Principle 2: Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

All relevant databases, which hold personal information about living individuals, must be registered with the Office of the Information Commissioner. This process is known as notification. The Head of Information Governance will complete this process and keep the information up to date on behalf of the organisation.

The organisation will produce patient/service-user information leaflets describing the uses of patient information (as described above) and will inform staff what information is held about them, how this is used and to whom it may be disclosed.

The organisation will ensure that information sharing protocols are in place to ensure that personal data that is passed on is used only for the specified purposes as notified to the Information Commissioner.

Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

The organisation will ensure that records management policies and procedures are in place to support the gathering of relevant, adequate information that is not excessive for its purposes.

The organisation will ensure that systems and processes ensure only relevant information is captured and processed. The organisation will implement ‘need to know’ access controls and will conduct routine audits as part of good data management practice.

Principle 4: Personal data shall be accurate and, where necessary, kept up to date

All staff who record data are responsible for its quality (that is, accuracy, timeliness, and completeness).

It is the responsibility of each member of staff to notify their organisation of any changes in their personal circumstances, for example, change of address.

Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
The organisation will ensure that records management policies and procedures are in place, including processes for records appraisals so that records are not kept for longer than necessary. Full details of how this principle affects the organisation, and actions required to comply with it, are set out in the Records Management Policy and Records Management Schedule of Retention and Disposal. These documents detail disposal arrangements for the, archiving, closure and destruction of records.

**Principle 6: Personal data shall be processed in accordance with the rights of data subjects under this Act**

Under the Data Protection Act, individuals have the following rights:

- right of subject access
- right to prevent processing likely to cause harm or distress
- right to prevent processing for the purposes of direct marketing
- right in relation to automated decision taking
- right to take action for compensation if the individual suffers damage
- right to take action to rectify, block, erase or destroy inaccurate data
- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

A procedure for handling requests for access to personal information and health records is set out in the Subject Access Policy.

**Principle 7: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**

Whilst recognising the diversity of people, working practices, the application of technology across the organisation/its partner organisations, the organisation will have in place an Information and IT Security policy, together with associated system-specific security policies and procedures to ensure Information is protected.

The organisation will ensure that a Records Management policy and associated procedures are in place setting out measures to protect current and archived records.

The organisation will ensure that the sharing of personal identifiable information, data and software exchange conforms to protocols, including disclosure in line with statutory requirements. The details of this are set out in of the Information and IT Security Policy.

**Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory**
ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

This principle is not infringed if the explicit informed consent of the individual is obtained for the transfer and can be evidenced. An exception to this would be where one clinician transfers clinical information to another clinician in the vital interests of a patient. Details of EEA can be found on ICO website. www.ico.gov.uk

Appendix 2

EXEMPTIONS TO THE DATA PROTECTION ACT 1998

Disclosing information against an individual’s wishes

Personal information must not be disclosed to third parties without informed written consent except in very limited circumstances. In these circumstances an assessment of the need to disclose the information against an individual’s wishes must be made. The details of this assessment must be documented together with details of what information has been released and to whom.

The responsibility of whether or not information should be withheld or disclosed without the subject’s consent lies with the senior manager or senior clinician involved at the time and cannot be delegated. Circumstances where a person’s right to confidentiality may be overridden are rare.

Examples are as follows:

- where a patient’s life may be in danger, or in cases where a patient may not be capable of making an appropriate decision
- where there is serious danger to other people, where the rights of others may supersede those of the patient
- where there is serious threat to the community
- in other exceptional circumstances, based on professional consideration and consultation

The following are examples of where disclosure without consent is permitted:

- births and deaths
- notifiable communicable diseases
- poisonings and serious accidents in the workplace
- terminations of pregnancy
- offenders thought to be mentally disordered
- child abuse
- road traffic accidents
- prevention/detection of a serious crime

The Department of Health publication Confidentiality: NHS Code of Practice (2003) provides a decision support tool to aid decision-making about the use or disclosure of confidential patient information. If in doubt, staff must seek
guidance from the appropriate senior manager/clinician or from the Caldicott Guardian or Information Governance. In complex cases the organisation will seek expert guidance from legal advisers.

Appendix 3
Caldicott Principles for handling patient-identifiable information

The Caldicott principles

- **Principle 1: Justify the purpose(s)**

  Every proposed use or transfer of patient identifiable information within or from an NHS organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the Caldicott Guardian.

- **Principle 2: Don’t use patient identifiable information unless absolutely necessary**

  Patient identifiable information items should not be used unless there is no alternative.

- **Principle 3: Use the minimum necessary patient identifiable information**

  Where use of patient identifiable information is considered to be essential use only that information necessary to achieve the purpose.

- **Principle 4: Access to patient identifiable information should be on a need to know basis**

  Only those individuals who need to access patient identifiable information should have access to it, and they should only have access to the information items they need to see.

- **Principle 5: Everyone 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 aware of their responsibilities and obligations to respect patient confidentiality.

- **Principle 6: Understand and comply with the law**

  Every use of patient identifiable information must be lawful.
Appendix 4

General Guidance

Safe Haven Arrangements

The Department of Health publication *Confidentiality: NHS Code of Practice* states that “care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are as secure as they can be”.

The term ‘safe haven’ was originally implemented to support contracting procedures. Nowadays a ‘safe haven’ refers to a location (or a piece of equipment) on the organisation premises where a set of administrative arrangements are in place to ensure the safe and secure handling of confidential information - including personal information - between sites. It covers a range of media, for example, backup electronic storage devices, telephones, message boards, answering machines and post.

The organisation will set out ‘safe haven’ procedures to maintain the privacy and confidentiality of personal information held.

When information is transferred via a ‘safe haven’ point to an equivalent ‘safe haven’ staff can be confident that agreed protocols will govern the use of information from the transmitting ‘safe haven’ to the recipient ‘safe haven’.

All staff will be trained in the use of ‘safe haven’ facilities at the organisation’s sites where person and patient identifiable information is being transferred.

Safe Haven Facsimile (Fax) Machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. Only the minimum amount of personal information must be sent. Where possible the information should be anonymised or a unique identifier used.

Only those fax machines designated as safe havens may be used for the transmission and receipt of person or patient identifiable information. The organisation will maintain a list of safe haven fax facilities in use. Formal application for a safe haven fax must be made to Information Governance.

Security arrangements for Safe Haven Fax facilities set out as follows:

- the fax machine is designated by the organisation as a ‘safe haven fax’
• the fax machine will be located in a room (or cupboard) where only authorised staff can enter and other members of staff, or visitors, cannot see faxes received

• if sited on a ground floor then windows will be fitted with window locks

• the room will conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage

• the room will be lockable and will be locked when not in use or access to the room will be via a coded key-pad known only to authorised staff

• if an unauthorised person requires access to the room they must be accompanied

• the fax machine will only be operated by a fully trained member of staff

• all items of faxed mail must be marked SAFE HAVEN and have a confidentiality notice on the cover sheet

When transmission of person or patient identifiable information by fax is essential, and the recipient cannot guarantee safe haven facilities, the following practice and principles should be followed:

• transmit only from a designated Safe Haven fax

• ensure that the fax is sent to a location where only staff that have a legitimate right to view the information can access it

• use a fax cover sheet which makes clear that the information contained in the fax is confidential and should only be read by the intended recipient.

• fax to a named person and check that the fax number is correct

• key in the fax number and check before selecting start or send button

• ensure someone is at the receiving end waiting for the fax

• notify the recipient when you are sending the fax and ask them to confirm receipt of message by telephone

• obtain a successful delivery receipt from the fax machine and keep with original fax

**Bulk Transfers of Patient or Personal Identifiable Information/Data**

Any/all requests for batch data, reports or lists which include patient or person-identifiable information, must be made directly to Information Services to ensure
that Information Governance arrangements are in place and assured. A bulk transfer is described as relating to 50 or more individuals.

**Sending Personal Confidential Information by Post**

Royal Mail Services are permitted for direct patient care, for example, sending a patient an appointment card. Written communications containing personal information must be transferred in a sealed envelope and addressed, by name, to the recipient. Written communications to patients must not be marked ‘NHS Confidential’. Managers must carry out individual risk assessments on sending more sensitive information or multiples and document the same outlining why they have made the decision.

**Transporting Personal Confidential Information Internally**

Health records, and internal written communications containing personal confidential information, must be transferred in a sealed envelope (preferably a polylopes) or container and addressed, by name, to the recipient for whom it is intended. That is, a postholder, a person or a legitimate safe haven, but never to a department, a unit or an organisation. Where mail is for a team, it should be addressed to an agreed postholder or team leader. Such communications should be marked ‘NHS Confidential’.

The classification ‘NHS Confidential’ will be used for patients’ clinical records and patient identifiable clinical information that moves between NHS staff and between NHS staff and staff of other appropriate agencies. The name and address of the sender must be clearly marked on the back of the envelope. Transit envelopes must not be used.

The designated person must be alerted to the despatch of such information and should make arrangements to ensure both that the envelope is delivered to them unopened and that it is received within the expected timescale.

Internal post must be transported securely between sites to protect confidential information from loss or accidental viewing.

Any losses must be reported immediately to the organisation’s Risk Manager using an IR1 and to the Information Governance team

**Use of Secure Courier Services for the Transfer of Person or Patient Identifiable or Sensitive Information**

The organisation will draw up a list of trusted and reliable courier services for such transfers.

A secure courier service must be used where additional security is needed. The use of a secure courier will allow the item to be taken directly from its pick-up point to the destination and signed for at each end. The authority to use a courier services must be obtained from the departmental heads or heads of service. The recipient must be informed that a transfer will take place via a courier service.
Use of Taxi for the Transfer of Person or Patient Identifiable Information

The use of a taxi for such a transfer of information must be rare and reserved for documents requiring immediate transfer locally. The authority to use a taxi for such a transfer must be obtained by a departmental head or head of service. The following security arrangements must be in place:

- Use only one use polylopes-do not use transit envelopes
- address to a named recipient and mark ‘NHS Confidential – to opened by the named recipient only’
- write name and address of sender on the back of the envelope
- seal and sign on flap of envelope
- tape over signature and flap
- inform recipient by phone when taxi leaves
- obtain confirmation from recipient that all packages have arrived intact upon arrival.

Email

Managers will ensure that all staff are aware on commencement that staff are aware of the Email and Internet Usage Policy and have signed the annual Information Governance Code of Confidentiality Policy. In addition it should be enforced that email is not a secure system and that person or patient identifiable or other sensitive information must not be sent by email unless it is encrypted to standards approved by the NHS.

Confidential Information and the Media

The work of the organisation involves confidential matters. Any member of staff contacted by the media about any matter relating to the press must refer all such enquiries to locality communications lead.

The organisation will not make comment in response to media enquiries on individual cases that may breach the individual’s statutory rights to confidentiality or the organisations statutory rights to maintain it. The Caldicott Guardian will advise on all matters where patient information is in the public domain, for example, where an individual case may be named in the enquiry or reported by the media.
Appendix 5

GLOSSARY OR TERMS/LEGISLATION AND GUIDANCE

NHS West Lancashire CCG staff have a legal obligation to comply with the following:

The Common Law Duty of Confidentiality

This means that information given in confidence must not be disclosed without a person’s consent unless there is a valid justifiable reason such as a requirement of a statute of law or it is judged that there is an overriding public interest to do so.

The Data Protection Act 1998

The Data Protection Act puts strict controls on the use of personal information, in order to enforce this, the Chief Officer has overall responsibility for compliance and is designated the data Controller. The implementation for compliance is delegated to the CCG SIRO and Head of Information Governance CSU and other designated staff. Personal data is classed as information that can identify a living individual. It covers all computerised and paper records and in fact can cover all forms of personal information that is recorded i.e. – X-rays, CCTV, photographic images. The Act’s eight principles Act are shown in appendix 1.

The Caldicott Report

This is a report undertaken by the Caldicott Committee on behalf of the Department of Health in 1997. The report made a number of recommendations on the use and disclosure of patient-identifiable information, which NHS organisations have to implement (see appendix 2 for more information). The report required each organisation to identify and appoint a Caldicott Guardian, who should be a senior health professional to oversee and ensure compliance.

Professional Codes of Conduct

All health professionals must adhere to their professional codes of conduct, which include significant sections on patient confidentiality.

Human Rights Act 1998

This sets out basic human rights for people – one of which is the right to privacy. All public bodies have to make sure their activities comply with the stated rights.

NHS Code of Practice: Confidentiality

This Department of Health publication gives NHS staff detailed guidance on rules and legislation governing the use and disclosure of patient information. It
also includes a number of flow charts to assist staff to make decisions on confidentiality and disclosure.

**The Health and Social Care Act 2001 (section 60)**

Section 60 gives the Secretary of State Powers to permit the use of patient data in certain special cases without the necessity of gaining consent. A recent example of these powers has been to allow disclosure of patient data to support activities for cancer registries.

Requests by persons or agencies who wish to gain access to patient data without obtaining consent will need to apply to the Patient Information Advisory Group (PIAG) who can advise the Secretary of State on such matters. This may affect researchers wishing to use the organisation’s patient data.

**Freedom of Information Act 2000**

The Act came into full effect on 1st January 2005 and from this date the majority of publicly recorded information held by the organisation will be accessible to anyone. Documents this may affect include accounts, reports, policies, procedures and certain minutes of meetings.

Where information that has been requested contains personal information, disclosure of those details will only be permitted if data protection conditions are met.

**Public Interest Disclosure Act 1998 (“Whistle blowing”)**

This Act gives employees certain legal protection against dismissal or being penalised by their employer where they disclose information, which may show malpractice within their organisation.

Staff should consult the Whistle Blowing Policy: before considering any such disclosure, be aware of the mechanisms of the internal procedure, and also what type of disclosure is covered by the Act.

Breaches of the above may lead to disciplinary action for staff or the imposition of heavy fines on the organisation. A health professional can be struck off if they break their professional code of conduct.

A breach of confidentiality has the potential to damage the reputation, credibility and good standing of the organisation.