Equality Impact Assessment
In applying this policy, the organisation will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic. A single Equality Impact Assessment is used for all policies and procedures.

This document has been assessed to ensure consideration has been given to the actual or potential impacts on staff, certain communities or population groups.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Aims</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Scope</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Accountability and Responsibilities</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Definitions of Terms</td>
<td>6</td>
</tr>
<tr>
<td>5.1</td>
<td>Personal Confidential Data</td>
<td>6</td>
</tr>
<tr>
<td>5.2</td>
<td>Sensitive Personal Data</td>
<td>6</td>
</tr>
<tr>
<td>5.3</td>
<td>Corporate Information</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>Confidentiality Code of Practice, Guidance and Legislation</td>
<td>7</td>
</tr>
<tr>
<td>6.1</td>
<td>Data Protection Act 1998</td>
<td>7</td>
</tr>
<tr>
<td>6.2</td>
<td>Human Rights Act 2000</td>
<td>8</td>
</tr>
<tr>
<td>6.3</td>
<td>Common Law Duty of Confidentiality</td>
<td>8</td>
</tr>
<tr>
<td>6.4</td>
<td>Caldicott Principles</td>
<td>8</td>
</tr>
<tr>
<td>6.5</td>
<td>Health and Social Care Information Centre (HSCIC) Guidance</td>
<td>10</td>
</tr>
<tr>
<td>6.6</td>
<td>NHS and Social Care Record Guarantees for England</td>
<td>10</td>
</tr>
<tr>
<td>6.7</td>
<td>NHS Act 2006</td>
<td>10</td>
</tr>
<tr>
<td>6.8</td>
<td>Computer Misuse Act 1990</td>
<td>11</td>
</tr>
<tr>
<td>6.9</td>
<td>Other Legislation and Guidance</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Ensuring Information is Confidential and Secure</td>
<td>12</td>
</tr>
<tr>
<td>7.1</td>
<td>General Principles</td>
<td>12</td>
</tr>
<tr>
<td>7.2</td>
<td>Using and Disclosing Confidential Patient Data for Direct Healthcare</td>
<td>12</td>
</tr>
<tr>
<td>7.3</td>
<td>Using and Disclosing Confidential Staff information</td>
<td>13</td>
</tr>
<tr>
<td>7.4</td>
<td>Using and Disclosing Corporate and Business Information</td>
<td>13</td>
</tr>
<tr>
<td>7.5</td>
<td>Information Security</td>
<td>13</td>
</tr>
<tr>
<td>7.6</td>
<td>Sharing Confidential Information without Consent</td>
<td>13</td>
</tr>
<tr>
<td>7.7</td>
<td>Confidentiality and Conversations</td>
<td>14</td>
</tr>
<tr>
<td>7.8</td>
<td>Records Management</td>
<td>14</td>
</tr>
<tr>
<td>7.9</td>
<td>Access to Records</td>
<td>14</td>
</tr>
<tr>
<td>7.10</td>
<td>Information Sharing</td>
<td>15</td>
</tr>
<tr>
<td>7.11</td>
<td>Information Confidentiality Breaches</td>
<td>15</td>
</tr>
<tr>
<td>7.12</td>
<td>Privacy Impact Assessment</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>Training</td>
<td>16</td>
</tr>
<tr>
<td>8.1</td>
<td>Mandatory Training</td>
<td>16</td>
</tr>
<tr>
<td>8.2</td>
<td>Specialist Training</td>
<td>16</td>
</tr>
<tr>
<td>9</td>
<td>Implementation and Dissemination</td>
<td>16</td>
</tr>
<tr>
<td>10</td>
<td>Monitoring Competence and Effectiveness of the Policy</td>
<td>17</td>
</tr>
<tr>
<td>11</td>
<td>Advice and Guidance</td>
<td>17</td>
</tr>
<tr>
<td>12</td>
<td>Associated Documents</td>
<td>17</td>
</tr>
</tbody>
</table>
CONFIDENTIALITY AND DATA PROTECTION POLICY

1. INTRODUCTION

NHS Leeds West Clinical Commissioning Group (CCG) recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The CCG also recognises the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which it processes, stores, shares and disposes of information.

Confidentiality and data protection legislation and guidance provide a framework for the management of all data from which individuals can be identified. It is essential that all staff and contractors of the CCG are fully aware of their personal responsibilities for information which they may come into contact with.

The policy incorporates the Confidentiality Code of Conduct (Section 6).

2. AIMS

The aim of the policy is to ensure that all staff understand their obligations with regard to any information they come into contact with in the course of their work and to provide assurance to the Governing Body that the CCG have in place the processes, rules and guidelines to ensure such information is dealt with legally, efficiently and effectively.

The CCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of Data Protection Act 1998 and other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Information Governance Toolkit.

This policy supports the CCG in its role as a Commissioner of Health Services and will assist in the safe sharing of information with its partner and agencies.

3. SCOPE

This policy must be followed by all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, pool staff, Governing Body members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the CCG. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy covers:

All aspects of information within the organisation, including (but not limited to):
- Patient/Client/Service User information
- Personnel/Staff information
- Organisational and business sensitive information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of, the organisation
- CCG information held on paper, floppy disc, CD, USB/Memory sticks, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- Transmission of information – verbal, fax, e-mail, post, text and telephone
- Sharing of information for clinical, operational or legal reasons
- The storage and retention of information
- The destruction of information.

Confidentiality and data protection within an independent contractor’s (such as GPs and Dentists) premises is the responsibility of the owner/partners. However, the CCG is committed to supporting independent contractors in their management of information risk and will provide advice, share best practice and provide assistance when appropriate.

The CCG recognises the changes introduced to information management as a result of the Health and Social Care Act 2012 and will work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

4. **ACCOUNTABILITY AND RESPONSIBILITIES**

There are a number of key information governance roles and bodies that the CCG needs to have in place as part of its Information Governance Framework, these are:

- Governing Body
- Assurance Committee
- Accountable Officer
- Senior Information Risk Owner
- Caldicott Guardian
- Information Asset Owner
- Information Asset Administrator
- Heads of Service
- All employees
The accountability and responsibility are set out in more detail in the Information Governance Strategic Vision, Policy and Framework which must be read in conjunction with this policy.

5. **DEFINITION OF TERMS**

The words used in this policy are used in their ordinary sense and technical terms have been avoided.

5.1 **Personal Confidential Data**

Personal confidential data (PCD) refers to all items of information in any format from which an individual might be identified or which could be combined with other available information to identify an individual and is information which has a duty of confidence.

This includes (but is not limited to):

- Name
- Date of Birth
- Post Code
- Address
- National Insurance Number
- Photographs, digital images etc.
- NHS or Hospital/Practice Number
- Date of death

5.2 **Sensitive Personal Data**

Certain categories of information are classified as sensitive personal data and additional safeguards are necessary when sharing or disclosing this information in line with guidance and legislation. This includes (but is not limited to):

- Physical and Mental Health
- Social care
- Ethnicity and Race
- Sexuality
- Trade union membership
- Political affiliations
- Religion
- Records relating to criminal charges and offences
5.3 Corporate Information

Corporate information includes the types of information listed below. Corporate information could be accessible through the Freedom of Information Act either from the CCG responding to a request for information or through making information accessible via the CCG Freedom of Information Publication Scheme. Where any corporate information has a duty of confidence attached to it - the information may be exempt from release. Additionally, other exemptions of the Act could restrict release of certain corporate information.

- Governing Body and meeting papers and minutes
- Tendering and contracting information
- Financial and statistical information
- Project and planning information

6. CONFIDENTIALITY CODE OF PRACTICE, GUIDANCE AND LEGISLATION

For personal and confidential Information held by the CCG there will be appropriate measures to ensure confidentiality and security, underpinning the principles of Caldicott, Health and Social Care Information Centre Guidance, professional Codes of Practice and legislation.

6.1 Data Protection Act 1998

All information and data which can identify a living person, held in any format (visual, verbal, paper, electronic, digital, microfilm, etc) is safeguarded by the Act, which is underpinned by eight principles.

The Act is enforced by the Information Commissioner’s Office. Fines can be made against organisations or persons holding personal information (data controllers) of up to £500,000 where is a serious breach of the Act e.g. loss of personal data of many individuals.

The Act requires data controllers such as the CCG to register on an annual basis with the Information Commissioners Office (Register of data controllers)

Data Protection Principles:

1. Personal data shall be processed fairly and lawfully

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.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

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

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.

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.

6.2 Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

There should be no interference with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

6.3 Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:

- Where the individual to whom the information relates has consented
- Where disclosure is in the public interest; and
- Where there is a legal duty to do so, for example a court order

6.4 Caldicott Principles

Dame Fiona Caldicott produced a report in 1997 on the use of patient information which resulted in the establishment of Caldicott Guardians across the NHS Structure. She was asked to conduct a further review and a new report: ‘Information to share or not to share’ was published in March 2013. The recommendations of this report have been largely accepted by the government.
and a revised set of Caldicott Principles have been published:

1. **Justify the purpose(s)**
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal Confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

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

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

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

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

7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Caldicott Guardian also has a strategic and operational role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation’s overall governance framework. A detailed description of the Caldicott Function is given in the Information Governance Strategic Vision, Policy and Framework.
6.5 Health and Social Care Information Centre (HSCIC) Guidance

This organisation was established in April 2013 and will be responsible for facilitating the management and sharing of data across the re-configured NHS to support both operational and other functions such as planning, research and assessments. HSCIC produced a Code of Practice: ‘A Guide to Confidentiality in Health and Social Care’ in September 2013:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of individuals.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual’s right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

6.6 The NHS and Social Care Record Guarantees for England

The NHS and Social Care Record Guarantees for England sets out the rules that govern how individual care information is used in the NHS and in Social Care. It also sets out what control the individual can have over this.

Individuals’ rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly with regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

6.7 NHS Act 2006

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

In late 2014, the government will introduce new regulations under this Act to support the sharing and use of information for defined commissioning activities and to support the new NHS structure subject to safeguards.
6.8 Computer Misuse Act 1990

This Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Access data or programs held on computer without authorisation. For example, to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
- Access data or programs held in a computer without authorisation with the intention of committing further offences, for example fraud or blackmail.
- Modify data or programs held on computer without authorisation.

6.9 Other legislation and guidance

In addition to the main legal obligations and guidance there are a wide range of Acts and Regulations which are relevant to data Protection and confidentiality which may have an effect on disclosure and use of information (see list below). This is not an exhaustive list. Where you need any further guidance regarding any of the legislation or guidance listed - you can contact the organisation’s Caldicott Guardian, the Senior Information Risk Owner (SIRO) or the Information Governance Support team (see section 11 Advice and Guidance).

- Health and Social Care Act 2012
- Crime and Disorder Act 1998
- The Children Act 1989 and 2004
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Electronic Communications Act 2000
- Public Interest Disclosure Act 1998
- Audit & Internal Control Act 1987
- NHS Sexually transmitted disease regulations 2000
- Human Fertilisation and Embryology Act 1990
- Abortion Regulations 1991
- Road Traffic Act 1988
- Regulations under Health and Safety at Work Act 1974
- Public Records Act 1958
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Protection of Freedoms Act 2012
- Coroners and Justice Act 2009
All staff are bound by the codes of conduct produced by any professional regulatory body, by the policies and procedures of the organisation and by the terms of their employment contract.

The Department of Health Records Management Code of Practice sets out guidance for the creation, processing, sharing, storage, retention and destruction of records.

7. **ENSURING INFORMATION IS SECURE AND CONFIDENTIAL**

7.1 **General Principles**

- The CCG regards all identifiable personal information relating to patients as confidential and compliance with the legal and regulatory framework will be achieved, monitored and maintained.
- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The CCG will establish and maintain policies and procedures to ensure compliance with the Data Protection Act, Human Rights Act, the Common Law Duty of Confidentiality and the Freedom of Information Act and Environmental Information Regulations and other related legislation and guidance.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable confidentiality and data protection controls are in place.
- Where any disclosure of PCD is made there a must be a legal basis for doing so.

7.2 **Using and Disclosing Confidential Patient Information for Direct Healthcare**

Consent to disclose can usually be taken to be implied when the information sharing is needed for direct healthcare but patients should still be informed about:

- The use and disclosure of their healthcare information and records.
- The choices that they have and the implications of choosing to limit how information may be used or shared.
- The breadth of the sharing necessary when care is to be provided by partner agencies and organisations.
- The potential use of their records for the clinical governance and audit of the care they have received.
7.3 Using and Disclosing Confidential Staff Information

Consent to disclose can usually be taken to be implied when the information sharing is needed for direct communications related to their role, salary payment and pension arrangements. Staff should be made aware that disclosures may need to be made for legal reasons, to professional regulatory bodies and in response to certain categories of freedom of information requested where the public interest in disclosure is deemed to override confidentiality considerations.

7.4 Using and Disclosing Corporate and Business Information

All staff should consider all information which they come into contact with through the course of their work as confidential and its usage and any disclosure would be in line with agreed duties and for authorised work purposes.

Corporate information could be accessible through the Freedom of Information Act either from the CCG responding to a request for information or through making information accessible via the CCG Freedom of Information Publication Scheme.

7.5 Information Security

Rules and guidance on information security are set out in

- The Information Security Policy - sets rules, guidance and good practice on ensuring security of information in the workplace, on areas such as portable devices, email, paper and electronic systems.
- The Records Management and Information Lifecycle Policy – includes sections on transfer of, storage and archival of records.

7.6 Sharing Confidential Information without Consent

It may sometimes be necessary to share confidential information without consent or where the individual has explicitly refused consent. There must be a legal basis for doing so (e.g. Safeguarding Children concerns) or a court order must be in place. In deciding on any disclosure certain considerations and steps need to be taken:

- Discuss the request with the appropriate CCG personnel such as the Caldicott the SIRO, Information Governance Specialist.
- Disclose only that information which is necessary or prescribed by law.
- Ensure recipient is aware that they owe a duty of confidentiality to the information.
- Document and justify the decision to release the information.
- Take advice in relation to any concerns you may have about risks of significant harm if information is not disclosed.
• Follow any locally agreed Information Sharing Protocols and national guidance.

Requests may be received by other agencies which are related to law enforcement such as:

• The Police or another enforcement agency where the appropriate section 29 request form (in line with the Access to Records Procedure) needs to be submitted from the law enforcement agency in order for the CCG to consider the request.
• The Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity.

Staff should also take into account the 2013 Caldicott Guidance such as:

The duty to share information can be as important as the duty to protect patient confidentiality.

7.7 Confidentiality and Conversations

Where during the course of your work you have conversations relating to confidential matters which may involve discussing (or disclosing information about) individuals such as staff members or patients you must ensure:

• That such discussions take place where they cannot be overheard.
• That for telephone calls the rule is you do not give out confidential information over the phone - unless you are certain as to the identity of the caller and they have a legal basis to receive such information (e.g. you may need to speak with another team member on the phone who is based at another location).
• Where you receive a request over the telephone for confidential information ask the caller to put the request in writing so details can be verified.
• That you do not discuss confidential work matters in public places or at social occasions.
• Where an answer phone is used ensure that recorded conversations on the phones cannot be overheard or otherwise inappropriately accessed.

7.8 Records Management

The CCG has a Records Management and Lifecycle Policy which should be followed for all aspects of record creation, sharing, storage, retention and destruction of records.

7.9 Access to Records

Individuals have a right to request access to their records in line with the Data Protection Act. All staff should familiarise themselves with the CCG’s Access to
Records Procedure which should be followed for all requests for personal data. This procedure also gives guidance in relation to requests for the records of deceased persons’ under the Access to Health Records Act 1990 and for dealing with requests for information from the police.

Access to corporate information and records will be in accordance with CCG’s Freedom of Information Act and Environmental Information Regulations Policy.

7.10 **Information Sharing**

The organisation will ensure that information sharing takes place within a structured and documented process and in line with the Information Commissioner’s Code of Conduct and the additional safeguards introduced by the Health and Social Care Act 2012.

Any local Information Sharing Protocols that the CCG is signed up to needs to be followed at all times.

7.11 **Information Confidentiality Breaches**

All actual, potential or suspected incidents involving breaches of confidentiality must be reported via the CCG’s Incident Reporting procedure. All incidents involving patient data should be reported to the Caldicott Guardian. The SIRO should consider whether serious breaches of confidentiality or those involving large numbers of individuals need to be reported to the Information Commissioner via the Information Governance Toolkit incident reporting tool. These types of incidents are known as Serious Incidents Requiring Investigation (SIRIs).

**What should be reported?**

Misuses of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again. The following list gives some examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to the computer systems either by staff or a third party.
- Unauthorised access to personal confidential personal information where the member of staff does not have a need to know.
- Disclosure of personal data to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality.
- Sending data in a way that breaches confidentiality.
- Leaving confidential information lying around in a public area e.g. photocopier.
- Theft or loss of patient-identifiable information.
Confidentiality and Data Protection Policy

• Disposal of confidential information in a way that breaches confidentiality i.e. disposing of patient records and or content of in an ordinary waste paper bin.

7.12 Privacy Impact Assessment

All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisation to address the privacy concerns and risks a technique referred to as a Privacy Impact Assessment (PIA) must be used. A PIA will:

• Identify privacy risks to individuals
• Protect the CCG’s reputation
• Ensure person identifiable data is being processed safely
• Foresee problems and negotiate solutions

The CCG procedure for the PIA should be followed.

8. TRAINING

8.1 Mandatory Training

The Information Governance Toolkit requires that all staff must undergo information governance training annually. All staff will receive information governance training via the CCG’s Statutory and Mandatory Training Programme.

Training will be delivered through the HSCIC Information Governance Training Tool.

Managers must actively ensure that all staff undertake and complete the mandatory information governance training.

8.2 Specialist Training

Additional training may be provided in specialist areas such as data protection. The need for additional training should be identified through the Personal Development Review process.

9. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Assurance Committee this policy will be disseminated to staff via the CCG’s intranet and communication through in-house staff briefings.

This policy will be reviewed every two years or in line with changes to relevant
10. **MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY**

An assessment of compliance with requirements, within the Information Governance Toolkit (IGT), will be undertaken each year. This includes confidentiality and data protection. Incidents are reported and all serious information governance issues must be reported by the SIRO at Governing Body level and in Annual Reports.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity by contacting the CCG Counter Fraud Specialist at the following link: [Counter fraud](#).

11. **ADVICE AND GUIDANCE**

Advice and guidance on any matters stemming from the Policy can be obtained by contacting:

[yhcs.infogov@nhs.net](mailto:yhcs.infogov@nhs.net)

12. **ASSOCIATED DOCUMENTS (Policies, protocols and procedures)**

This policy should be read in conjunction with:

- Information Governance Strategic Vision, Policy and Framework
- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Policy
- Disciplinary Policy
- Anti-Fraud Policy
- Anti-Bribery Policy
- Whistle Blowing Policy
- Internet and Email Policies and Procedures

And their associated procedures (including but not limited to):

- Access to Records Procedure
- Information Sharing Protocol
- Freedom of Information Procedures
• E mail and Internet Procedures
• Privacy Impact processes
• Remote access and home working procedures
• Safe Haven Procedure

This policy should also be read in conjunction with the Information Governance Handbook which provides guidance for staff on information governance compliance.