Bolton Clinical Commissioning Group

Confidentiality and Data Protection Policy

Policy Number	**IG002**
Target Audience	**CCG/GMSS Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**February 2018**
Last Review Date	**February 2018**
Next Review Date	**February 2020**
Policy Author	**GMSS IG Team**
Version Number	**V6.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1	September 2013	Approved	CCG Exec Team
1.1	January 2014	Andrea Hughes	Amendment to Section 3
	January 2014	IM&T Ops Board	Approved
1.2	November 2015	IG Team	Review document for approval
3.0	December 2015	IM & T Ops	Approved
4.0	January 2018	IG Team	Review document for approval, incorporating GDPR legislation
5.0	January 2018	IM & T Ops	Approved
6.0	February 2018	CCG Chief Officer	Approved.

Analysis of Effect completed	By: M Robinson	Date: August 2013

Contents

1 Introduction and aims

1.1. The purpose of this Policy is to provide guidance to all NHS Bolton Clinical Commissioning Group (referred to as "the CCG") employees on Data Protection.

1.2. The CCG has a statutory duty to safeguard the confidential information it holds, from whatever source, that is not in the public domain. The principle of this policy is that no individual or company working for or with the CCG shall misuse any information or allow others to do so.

1.3. During the course of their day to day work, many individuals working within or for the CCG will often handle or be exposed to information which is deemed personal, sensitive or confidential, (including commercially confidential) information. It is a requirement that any individual, company or other organisation to which this policy applies shall not at any time during the period they work for or provide services to the CCG nor at any time after its termination, disclose confidential information that is held or processed by the CCG.

1.4. All staff working in the CCG are bound by a common law duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of the Data Protection Act 1998 (henceforth referred to as DPA), the General Data Protection Regulation (henceforth referred to as GDPR) and, for health and other professionals, through their own professions' Codes of Conduct.

1.5. The CCG understands the need for the strictest confidentiality in respect of data. This applies to manual and electronic / computer records and conversations about service users' treatments. Everyone working for CCG is under a legal and common law duty to keep service users' information, held in whatever form, confidential.

1.6. The Information Commissioners Office (ICO) can impose penalties upon the CCG, and/or CCG employees if non-compliance occurs.

1.7. Confidentiality can only be overridden in exceptional circumstances and with the appropriate justification and be fully documented.

1.8. The CCG will ensure that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information where necessary;
- gain trust in the way the CCG handles information; and
- understand their rights to access information held about them.

1.9. It is the policy of the CCG that all processing of personal information by or on behalf of the CCG, whether as a Data Controller or as a Data Processor for others, shall be in accordance with the requirements of:

- Data Protection Act (DPA) 1998 and any subsequent amendments and statutory instruments;
- The General Data Protection Regulation
- the current Data Protection registration of the CCG;
- the CCG's Policies and Procedures in relation to the protection and use of personal information;
- processing personal information for deceased patients;
- the Access to Health Records Act 1990 and any subsequent amendments and statutory instruments.

1.10. The aims of this policy are:

- To safeguard all confidential information within the CCG;
- to provide guidelines for all individuals working within the organisation;
- to ensure a consistent approach to confidentiality across the CCG;
- to ensure all staff are aware of their responsibilities with regards to confidential information;
- to provide all individuals working within the CCG access to the documents which set out the laws, codes of practice and procedures relating to confidentiality and which apply to them. These include:

    - the common law Duty of Confidentiality;
    - Caldicott principles;
    - Data Protection Act 1998;
    - General Data Protection Regulation;
    - Freedom of Information Act 2000;
    - Human Rights Act 1998;
    - Department of Health's "Confidentiality: NHS Code of Practice" including supplementary guidance "Public Interest Disclosures";
    - The Public Interest Disclosure Act 1998;
    - The Computer Misuse Act 1990.

2 Scope

2.1. This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

2.2. For the purposes of this policy, confidential information shall include any confidential information relating to the CCG and/or its agents, customers, prospective customers, suppliers or any other third parties connected with the CCG and in particular shall include, without limitation:

- Service user information;
- ideas/programme plans/forecasts/risks/issues;
- trade secrets;
- business methods and business design;
- finance/budget planning/business cases;
- prices and pricing structures;
- sources of supply and costs of equipment and/or software;
- prospective business opportunities in general;
- computer programs and/or software adapted or used;
- policy advice and strategy;
- corporate or personnel information; and
- contractual and confidential supplier information.

2.3. This is irrespective of whether the material is marked as confidential or not.

3 The Current Data Protection Act / General Data Protection Regulation

3.1. These acts and regulations govern how we collect, store, process and share data. The Act dictates that information should only be disclosed on a need to know basis. The DPA is an Act of Parliament which defines UK law on the processing of data on identifiable living people. The DPA will be superseded by GDPR which comes into force May 2018.

3.2. The CCG has registered with the ICO as a data controller. A data controller must comply with the eight principles of the current DPA (please refer to section 4 of this policy) and the articles of the GDPR. The CCG is committed to compliance with the requirements of the DPA and GDPR and will ensure that all CCG employees and anyone providing a service on behalf of the CCG (directly employed and contractors) who have access to any personal data held by or behalf of the CCG), are fully aware of and abide by their duties and responsibilities of the Act and Regulation.

3.3. The CCG may be required by law to collect and use information about people with whom it works, including patients, public, employees, customers and suppliers. This personal information must be handled and managed appropriately however it is collected, recorded and used and whether it is a manual or electronic record.

3.4. DPA Principles / GDPR Articles(s)

3.4.1 The Current DPA defines eight data protection principles:

- DPA Principle 1 - Personal information shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

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

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

- DPA Principle 4 - Personal data shall be accurate and, where necessary kept up to date.

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

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

- DPA 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.

- DPA 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.

3.5. The new General Data Protection Regulation (GDPR)

3.5.1. The new GDPR doesn't refer to Principles however Article 5 contains requirements that are similar to the DPA Principles.

- (a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

  There is a requirement to make the general public aware of why the NHS needs information about them, how it is used and whom it may be disclosed to. The CCG is obliged under the DPA and Caldicott to produce a patient information leaflet. In order to meet the requirements of the first principle a clear policy of consent is also needed to ensure the requirements of the first principle is met.

- (b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes shall not be considered to be incompatible with the initial purposes;

Only use personal information obtained by the CCG in connection with the business of the CCG and ensure information is not used for any purposes other than originally intended.

- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

  Only obtain the minimum amount of information and do not obtain information which is not needed.

- (d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

  Ensure that all information entered either manually or electronically is accurate, and where recorded elsewhere ensure that there are appropriate procedures in place to continually review and update the different sources, to ensure accuracy and version control. Where possible do not hold duplicate copies as this increases the risk of inaccurate information being held

- (e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

  All records are affected by this article regardless of the media within which they are held and/or stored. For further guidance please see the CCG's Records Management Policy. When disposing of personal information use only the confidential waste destruction process.

- (f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

  Examples of which are:
  - Do not allow unauthorised access;
  - Do not share passwords and ensure you lock your PC screen before moving away;

- Do not leave confidential information on your desk/fax or post trays and ensure all paperwork is tidied away when not in use or at the end of the day.

3.6. Data Subject Rights

3.6.1. Data Subjects have enhanced rights under GDPR. In summary, data subjects still have the right to file a Subject Access Request (henceforth referred to as SAR) and obtain from the data controller a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, and the categories of third parties to whom the data may be disclosed.

3.6.2. The GDPR expands upon this right, requiring data controllers to respond to SARs with additional information, including details of the period for which the data will be stored (or the criteria used to determine that period) and information about other rights of data subjects. One major change to SARs relates to the charging of fees. Under GDPR the organisation will be unable to charge a fee for the processing of SAR's.

3.7. Transfer of data outside the EU

3.7.1. You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Please contact the IG team if you wish to transfer to an organisation/individual outside the EU

4 Accountability and Responsibilities

4.1. Chief Officer

4.1.1. Although it is the CCG that is the data controller, the Chief Officer has overall accountability and for the CCG's compliance with the DPA / GDPR.

4.1.2. The development, implementation of, and compliance with this policy is delegated to the Caldicott Guardian / SIRO and designated Data Protection Officer. The COO shall ensure that the CCG resubmits an annual data protection notification and fee to the Information Commissioners Office.

4.2. Responsibilities will be delegated to:

4.2.1. A Caldicott Guardian who will:

- ensure that the CCG satisfies the highest practical standards for handling personal identifiable/confidential information;

- act as the conscience of the CCG;
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information;
- represent and champion Information Governance requirements and issues at Board level;
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff;
- oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

4.2.2. A Data Protection Officer who will:

- inform and advise the CCG and its staff about their obligations to comply with the GDPR and other data protection laws;
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits;
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

4.2.3. A Senior Information Risk owner (SIRO) will:

- be an Executive Director or Senior Management Board Member;
- take overall ownership of the Organisations Information Risk Policy
- act as champion for information risk on the Board and provide advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk;
- understand the strategic business goals of the CCG and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed;
- work with GMSS (supplier of IG) to manage the NHS Information Governance risk assessment and management processes within the CCG;
- advise the Board on the effectiveness of information risk management across the CCG;
- receive training as necessary to ensure they remain effective in their role as SIRO.

4.2.4. Information Asset Owners (IAO) will (under the responsibility of the SIRO):

- will be identified, provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised users who require the access; ensure the integrity of the information within their area - know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset;
- know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy;
- will be responsible for the Information Asset assigned to them;

- understand and address risks to the asset, and providing assurance to the SIRO;
- will ensure that all personal data can be at all times obtained promptly from the Information Asset when required to process a Subject Access Request (SAR);
- will ensure that personal data held in the Information Asset is maintained in line with the CCGs Record Management Policy, specifically around maintaining the accuracy, validity and quality of the personal data. Any personal data when no longer required should be removed promptly in line with policy.

4.2.5. Information Governance Team (support provided by Greater Manchester Shared Services, GMSS) will:

- manage the Information Governance Team to deliver Information Governance for the CCG;
- maintain an awareness of information governance issues within the CCG;
- review and update the information governance policy in line with local and national requirements providing template documents to the CCG;
- ensure that line managers are aware of the requirements of the Information Governance policy.

4.2.6. Line managers will;

- take responsibility for ensuring that their staff are compliant with, and working to, all relevant policy and procedure in relation to Data Protectionthe DPA / GDPR
- where a breach of policy/procedure or near miss occurs, line managers will need to comply with the CCG Incident Management processes;
- line managers will ensure that anyone providing a service on behalf of the CCG (directly employed and contractors) completes a confidentiality statement before commencing employment.

4.2.7. All Staff (refers to all CCG employees including contractor/temporary staff and work place students) will:

- adhere to this policy and all related Information Assets and processes to ensure compliance with the DPA / GDPR;
- are subject to DPA / GDPR compliance and accountable via personal liability;
- have a responsibility to inform the GMSS IG Team of any new use of personal data immediately; must maintain an appropriate level of awareness of the DPA / GDPR and to attend training as appropriate;
- ensure that all personal information is accurate, relevant, up-to-date and used appropriately, for both electronic and manual Information Asset;
- ensure that personal data is not removed from the CCG premises except where specifically required for the execution of legitimate functions of the CCG and, then, only in accordance with appropriate policies;

- ensure that all copies of personal data output, or obtained from the system whether electronic, recorded on paper, microfilm, or any other form, are securely and confidentiality managed and destroyed/erased when they are no longer required for CCG purposes;
- ensure that the GMSS IG Team is advised as soon as possible of any problems or complaints relating to any SAR or unauthorised disclosures/ breaches of confidentiality;
- failure to adhere to this policy and its associated procedures may result in disciplinary action.

5 Conduct

5.1. Individuals shall not be restrained from using or disclosing any confidential information which:

- They are authorised to use or disclose by the CCG and/or;
- has entered the public domain unless it enters the publicdomain as a result of an unauthorised disclosure of an individual and/or;
- has entered the public domain by an authorised disclosure for an unauthorised purpose by the individual or anyone else employed or engaged by the CCG and/or;
- they are required to disclose by law; and/or;
- they are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regards to the provisions of that Act.

5.2. All individuals must:

- they are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regards to the provisions of that Act.
- Exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- ensure the physical security of all confidential documents and/or media, including storage of files on PCs. Confidential information must never be unattended and should be secure when not in use;
- use password protection and not disclose passwords to anyone including work colleagues;
- have regards to the provisions of that Act.

5.3. All individuals will be required to comply with this policy whilst working within the CCG and therefore for as long as the information remains confidential information. It is only when the information has entered the public domain that the information can no longer be classed as confidential.

5.4. If an individual is unclear if information should be classed as confidential, they must discuss the issue with their line manager who will offer advice.

6 The Duty of Confidence

6.1 All NHS bodies and those carrying out functions on behalf of the NHS have a duty of confidence to service users and a duty to support professional ethical standards of confidentiality.

6.2. Everyone working for the NHS that handles, stores or otherwise comes across information that is capable of identifying individual service users has a personal duty of confidence to the service user and to his/her employer.

6.3. The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

6.4. Service users expect that information given by them to their doctors, nurses and other members of the healthcare team is treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as staff. Particular care must be taken to avoid inadvertent or accidental disclosure.

The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised staff includes those who are not involved in either the clinical care of the service user or the associated administration processes.

6.5. No personal information, given or received in confidence, may be passed to anyone else without the consent of the provider of the information. This is usually the service user but sometimes another person may be the source (e.g. relative or carer).

6.6. No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information.

6.7. Service users are entitled to object to the use of their personal health data for purposes other than their immediate care.

6.8. The duty of confidentiality owed to a deceased service user must be viewed as being consistent with the rights of living individuals

7 Personal, Confidential and Sensitive Information

7.1. Like the current DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

7.2. Personal identifiable information, or personal data, is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition..

7.3. Information that identifies individuals personally must be regarded as confidential, and must not be used unless absolutely necessary.

7.4. Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified purposes.

7.5. Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.

7.6. Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive personal information (as defined by the –DPA / GDPR) regarding race, health, sexuality, etc.

7.7. Confidential information may be known, or stored on any medium. Photographs, videos, etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.

7.8. The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9). These categories are broadly the same as those in the DPA, but there are some minor changes.

7.9. Sensitive/confidential data under the terms of the DPA / GDPR includes but is not restricted to:

- Demographics, e.g. Name, address, date of birth;
- information about a person’s racial or ethnic origin;
- political opinions;
- gender;
- religion and belief;
- membership of a trade union;
- sexual life;
- criminal convictions or charges;
- any other information which may identify an individual.

8 Subject Access Request

8.1. A Subject Access Request, commonly referred to as a SAR, is a request from a data subject to see a copy of, personal information that is held about them as an organisation. All data subjects have the right (subject to exemptions) to access personal information which is kept about them by the CCG, both in electronic and paper files, this is known as a Subject Access Request (SAR).

8.2. Any individual is entitled to:

- Know what information is held about them and why;
- gain access to it regardless of the media which it is held;
- have their information kept up to date;
- require the CCG rectify/block, erase or destroy inaccurate information;
- not have processed confidential information about them likely to cause damage or distress;
- not have processed confidential information about them for the purposes of direct marketing.

8.3. In most cases the CCG will only process personal information with the consent of the data subject. If the information is sensitive, explicit consent may be needed. It may be a condition of patients, and employment of staff, that they agree to the CCG processing of specific classes of personal information.

8.4. The CCG may sometimes process information that by this definition is classed as sensitive. Such information may be needed to ensure safety, or comply with the requirements of other legislation.

9 Freedom of Information

9.1. The Freedom of Information Act 2000 widens the scope of the DPA / GDPR Data Protection Act and as it also makes provision for personal data to be disclosed to third parties providing none of the DPA Principles / GDPR Articles are breached. Information generally will not be disclosed if to do so would be regarded as a breach of confidentiality or if it would cause distress to the data subject.

9.2. This Act allows public access to information held by Public Authorities. Public authorities include government departments, local authorities, the NHS, state schools and police forces. However, the Act does not necessarily include every organisation that receives public money, e.g. it does not cover some charities that receive grants and certain private sector organisations that perform public functions.

9.3. The Act does not give people access to their own personal data (information about themselves) such as health records or credit reference file. If a member of the public wants to see information that a public authority holds about them then they should make a Subject Access Request (SAR).

10 Disclosing Information

10.1. The CCG must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances the Police. All staff and individuals providing a

service on behalf of the CCG should exercise caution when asked to disclose personal data held on another individual to a third party. Where an individual is unsure as to the legitimacy of disclosing information, the Line Manager or GMSS IG Team should always be consulted.

10.2. There may be times when personal data may be legitimately be disclosed, for example where:

- The individual has given their consent for information about them to be disclosed;
- the disclosure is in the legitimate interests of the provision of healthcare (e.g. if members of staff require the information to enable them to perform their jobs adequately or if there are justifiable patient safety concerns);
- the CCG is legally obliged to disclose the data.

10.3. The NHS Confidentiality: Code of Practice provides advice on using and disclosing confidential service user information and has models for confidentiality decisions and all staff should adhere to this guidance.

10.4. Personal information may be disclosed on the basis of informed consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality.

10.5. The CCG will inform service users, staff and any other data subjects why, how and for what purpose personal information is collected, recorded and processed.

10.6. Consent of the data subject will be required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

10.7. Under common law, personal information may be disclosed without consent for example:

- In order to prevent serious harm;
- where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.

10.8. Where information is required by the police CCG staff should consult the GMSS Information Governance Team.

11 Human Resources (HR) and Personnel Information

11.1 In keeping with good Human Resources practice, The CCG retains and processes personal data on its employees. In addition, the CCG may from time to time, retain and process "sensitive personal data" as defined by the DPA / GDPR for example in relation to sickness and occupational health records,
performance reviews, equal opportunities monitoring, for the prevention of fraud or other illegal activities.

11.2. The CCG may process such data and such data may be legitimately disclosed to appropriate employees and to CCG professional advisors, in accordance with the principles of the DPA and articles of the GDPR.

11.3. The CCG takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/ her may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with Human Resources.

12 Training and Awareness

12.1. The SIRO has the overall responsibility for ensuring that all staff are made aware of the requirements of the DPA / GDPR and their IG obligations and this will be carried out by regular mandatory Information Governance training sessions. Any new staff members (including temporary, contractors) will be required to complete Information Governance as part of their induction.

12.2. Information Governance training is required to be undertaken by all CCG employees and those providing a service to the CCG. All NHS staff are mandated to undertake annual Information Governance training.

12.3. Where staff have specific Information Governance roles within the CCG i.e. Caldicott Guardian, SIRO etc. additional Information Governance training will be required. Additional training will be made available to all persons, where it is required. For further guidance refer to the Information Governance Training Needs and Analysis (TNA) document.

12.4. To maintain high staff awareness the CCG will direct staff to a number of sources:

- Policy/strategy and procedure;
- Manuals;
- line manager;
- specific training courses;
- other communication methods, for example, team meetings; and staff Intranet.

13 Disciplinary

13.1. No employee shall knowingly misuse any information or allow others to do so.

13.2. Users must not access records/information that they have no legitimate reason to view, this includes records about themselves their family, friends, neighbours, acquaintances. If there is not a legitimate reason to access information users must not browse and should remember all transactions are auditable.

13.3. If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, he or she must report it immediately to their line manager and/or to the CCG Information Governance Team.

13.4. Breaches of Data Protection and Confidentiality are a serious matter and a breach of could result in dismissal and/ or prosecution.

14 Monitoring Review

14.1 This policy will be monitored through staff awareness and supporting evidence to the NHS IG Toolkit

14.2 This policy will be reviewed every two years, and in accordance with the following on an as when basis if the following occurs::

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities
- changes to organisational infrastructure.

14.3. Where there are no significant alterations required, this Policy shall remain for a period of no longer than two years of the ratification date.

15 Legislation

15.1. Legal Acts:

- Data Protection Act 1998;
- General Data Protection Regulation;
- Human Rights Act;
- Freedom of Information Act 2000;
- Thefts Act (1968 and 1978);
- Police and Criminal Evidence Act 1984 (PACE);
- Copyright, Designs and Patents Act (1988);
- Computer Misuse Act (1990);
- Trademarks Act (1994);
- Terrorism Act (2000);
- Proceeds of Crime Act (2002);
- Money Laundering Regulations (2007);
- Criminal Justice and Immigration Act (2008);
- Environmental Information Regulations;

- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act;
- Health and Social Care Act 2006 and ;
- Human Rights Act 1998.

15.2. Supporting Documents

- NHS Information Governance: Guidance on Legal and Professional Obligations;
- NHS Code of Confidentiality;
- Information Security Management: NHS Code of Practice April 2007;
- Caldicott Guardian Manual 2017;
- NHS Information Risk Management;
- Records Management Code of Practice for Health and Social Care 2016; (produced under S46 of the Freedom of Information Act 2000);
- The Information Governance Toolkit;
- Caldicott 3.

16 Other relevant Procedural Documents

- IG012 Secure Transfer of Information Procedure
- IG001 Information Governance Policy
- Freedom of Information Policy
- Information Security Policy
- Disciplinary Policy and Procedure

This list is not exhaustive and further IG policies and procedures can be found on the CCG's website.