NHS
Wigan Borough
Clinical Commissioning Group

Data Security, Protection & Confidentiality Policy

DOCUMENT CONTROL PAGE	
Title	Data Security, Protection & Confidentiality Policy 2018
Supersedes	Confidentiality and Data Protection Policy 2017
Minor Amendments	Amendments made to comply with the General Data Protection Regulation 2016 and the Data Protection Act 2018
Author	Lisa Winstanley / Chris Lawless (Greater Manchester Shared Services)
Ratification	IGOG – May 2018 Corporate Governance Committee – December 2018
Application	All Staff
Circulation	All Staff
Review	December 2020
Date Placed on the Intranet/SharePoint: Following Approval	**EqIA Registration Number** **16/13**

Contents

Introduction

1. NHS Wigan Borough Clinical Commissioning Group (henceforth referred to as "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.

2. The CCG holds confidential information relating to service users, staff and the organisation itself. This information should be treated with respect to ensure confidentiality, integrity and protect it from inappropriate disclosure and to make sure that it is not available to persons unauthorised to see it.

3. 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 2018(henceforth referred to as the DPA) and the General Data Protection Regulation (henceforth referred to GDPR) and, for health and other professionals, through their own professions' Codes of Conduct.

4. The CCG places great emphasis on the need for the strictest confidentiality in respect of personal data. This applies to manual and electronic records and verbal conversations. Everyone working in the CCG is under a legal and common law duty to keep service users' information held in whatever form, confidential.

5. The CCG is committed to the delivery of a first class confidential service. This means ensuring 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;
    - Understand their rights to access information held about them.

6. It also give assurance to the CCG and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

7. The CCG will establish and maintain policies and procedures to ensure compliance with requirements contained in the Data Security & Protection Toolkit (DSPT) and the Caldicott Reports.

8. 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:

    - The Data Protection Act (DPA) 2018 and any subsequent amendments and statutory instruments;
    - The General Data Protection Regulations (GDPR) 2016;
    - The legal requirement to pay a data protection fee (under the Digital Economy Act 2017) to the ICO;
    - 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.

Purpose

9. This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility.

10. 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.

11. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

12. The purposes 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.

13. 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.

14. Everyone working for the NHS has a personal duty of confidence to the service user and to his / her employer.

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

Data Protection Act 2018 / GDPR 2016

16. The Data Protection Act 2018 (DPA) along with the General Data Protection Regulation (GDPR) governs how we collect, store, process and share data.

17. GDPR is applicable throughout the UK from 25th May 2018 in conjunction with the Data Protection Act 2018 which was enacted on 23rd May 2018. The Data Protection Act 2018 fills in the gaps where flexibility and derogations are permitted in the UK. It will ensure that the provisions in the GDPR will be applicable in the UK post Brexit. It is important to note that the DPA 2018 does not replicate all the provisions in the GDPR but cross-refers therefore it is necessary to view both side by side in order to see the complete picture of all data protection legislation.

18. Under GDPR, the CCG no longer has to register with the ICO but under the Charges and Information Regulations 2018 (Digital Economy Act 2017) it will remain a legal requirement for data controllers to pay the ICO a data protection fee. These fees will be used to fund the ICO's data protection work.

19. The CCG who is a Data Controller, must comply with the 6 principles under 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 on behalf of the CCG or the Greater Manchester Shared Service (GMSS), are fully aware of and abide by their duties and responsibilities.

20. 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.

Principles relating to the processing of personal data

21. (***a) Processed lawfully, fairly and in a transparent manner in relation to individuals;***

The CCG must show transparency regarding how information is processed and the most common format of demonstrating this is via the production of a privacy notice. The CCG has a privacy notice available via the website which documents information processing activities.

22. ***(b) Collected for specified, explicit and legitimate purposes and not further processed in a matter 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.

23. ***(c) Adequate, relevant and limited to what is necessary in relation to the purposes of which they are processed;***

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

24. ***(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.

25. ***(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 interests, 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.

26. ***(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
- Do not leave confidential information on your desk or post trays and ensure all paperwork is tidied away when not in use or at the end of the day.
- Ensure that computer / laptop screens are locked when away from the desk.

Individual Rights

27. Individuals have strengthened rights under GDPR. In summary, these are:

- ***Right to access*** – individuals can request access to information we hold about them. The timeframe for responding with the information is 1 calendar month and no fee can be charged (unless exemptions apply). Under GDPR, organisations must now provide additional information about the processing of personal data when responding to a subject access request. In summary, this is an explanation of the categories of data being processed, the purpose of such processing, and the categories of third parties to whom the data may be disclosed. This is documented in the privacy notice so you can provide a copy of this on responding.
- ***Right to rectification*** – ask for inaccurate information to be corrected and must comply within one calendar month.
- ***Right to objection*** – individuals have the right to object to processing data about patients and staff. However, please note if we can demonstrate compelling legitimate grounds which outweighs the interest of you then processing can continue. If we didn't process any information about you and your health care (where the CCG process health data) it would be very difficult for us to care and treat you. Where this applies for direct marketing, this is an absolute right and in such cases the CCG must comply immediately and where automated processing used.
- ***Right to restriction on processing*** – individuals have right to restrict processing where accuracy is contested, data controller no longer needs data but subject requires it to be kept for legal claims and individual has objected pending verification of legitimate grounds and other national programmes such as NHS Digital national opt-out.
- ***Right to Data Portability -*** Only if we have your explicit consent for any processing we do, you have the right to have data provided to you in a format you have requested such as in an excel spreadsheet, csv file format.

- ***Right not to be subject to a decision based solely on automated processing -*** The CCG do not process data using this method, so this right will not apply to our data processing activities.

- ***Right to withdraw consent*** - You have the right to refuse (or withdraw) consent to information sharing at any time where we ask for consent. However, this may not be possible if the sharing is a mandatory or legal requirement imposed on the CCG. Any restrictions, and the possible consequences of withholding your consent, will be fully explained to you as the situation arises.

- ***Right to complain*** - If you feel that your personal data we hold at the CCG has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of personal data, please contact the Data Protection Officer and / or IG Team in the first instance to rectify this. If you are still unhappy with this response and wish to take your complaint to an independent body, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

Transfer of data outside the EU

28. 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.

Roles & Responsibilities

29. The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

30. The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements.

31. Responsibilities will be delegated to:

32. The Caldicott Guardian who will:

    - Ensure that the CCG satisfies the highest practical standards for handling patient identifiable information / 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 a senior management 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;

- At the CCG the post holder of Caldicott Guardian is the Associate Director of Quality and Safety.

33. The 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 Governing Body 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 the supplier of Information Governance to manage the NHS Information Governance risk assessment and management processes within the CCG;

- Advise the Governing Body on the effectiveness of information risk management across the CCG;

- Receive training as necessary to ensure they remain effective in their role as SIRO;

- At the CCG the post holder of SIRO is the Director of Transformation & Sustainability / Deputy Chief Finance Officer.

Data Protection Officer Role

34. The GDPR requires all public authorities to nominate a DPO. The role is a senior role with reporting channels directly to the highest level of management and has the requisite professional qualities and expert knowledge of data protection compliance. The role involves:

    - Advising colleagues on compliance;
    - Training and awareness raising;
    - Monitoring compliance and carrying out audits;
    - Providing advice regarding data protection impact assessments;
    - Being the main point of contact with the ICO;
    - Maintaining expert knowledge in data protection.

35. Information Asset Owners (IAO) will:

    - Lead and foster a culture that values, protects and uses information for the success of the CCG and benefit of its patient population;
    - 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 of information, and why, and ensure access is monitored and compliant with policy;
    - Understand and address risks to the asset, and providing assurance to the SIRO.

36. Information Governance Team 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 Data Security, Protection and Confidentiality Policy.

37. Line managers will take responsibility for ensuring that the Data Security, Protection & Confidentiality Policy is implemented within their group or directorate.

38. It is the responsibility of each employee to adhere to the policy.

39. Staff will receive instruction and direction regarding the policy from a number of sources:

    - Policy / strategy and procedure manuals;
    - Line manager;
    - Specific training course;
    - Other communication methods, for example, team meetings and staff Intranet.

40. All staff are mandated to undertake Information Governance training annually as identified in the CCG Information Governance Training Needs Analysis.

41. Where relevant further training and education will be required, staff will be informed via the Information Governance Training Needs Analysis.

The Duty of Confidentiality

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

43. Everyone working for or with NHS / CCG records who 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.

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

45. Service users expect that information given to them by 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 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.

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

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

48. The duty of confidentiality owed to a deceased service user is consistent with the rights of living individuals.

Caldicott Principles

49. In 2013, a second review was undertaken within the NHS regarding data processing following issues with information sharing and data losses. The principles are highlighted below and must be supported by the policies of their employers, regulators and professional bodies.

50. The 7 Caldicott Principles are:

51. ***Principle 1 – Justify the purpose(s) for using confidential information***

    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.

52. ***Principle 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).

53. ***Principle 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.

54. ***Principle 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.

55. ***Principle 5 – Everyone with access to personal confidential data should be aware of the 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.

56. ***Principle 6 – 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.

57. ***Principle 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 framework set out by these principles.

Confidentiality Codes of Practice

58. In 2013, the Health and Social Care Information Centre produced a document entitled 'A guide to confidentiality in health and social care – Treating confidential information with respect'. This outlines 5 rules that organisations should adhere to in relation to handling information.

These are:

59. **RULE 1**: Confidential information about service users or patients should be treated confidentially and respectfully

60. **RULE 2**: Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

61. **RULE 3**: Information that is shared for the benefit of the community should be anonymised.

62. **RULE 4**: An individual's right to object to the sharing of confidential information about them should be respected.

63. **RULE 5**: organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

64. Further guidance on the above rules can be found in the guidance document at: https://digital.nhs.uk/article/1226/A-Guide-to-Confidentiality-in-Health-and-Social-Care-

Definitions of Personal Data and Special Category of Data

Personal Data

65. Personal data is data that can identify an individual or with a combination of data items would identify an individual for example, name, address, postcode, date of birth, NHS number, National Insurance number etc. GDPR extends the definition of personal data to now include online identifiers and location data.

66. Information that identifies individuals is confidential, and should not be used unless absolutely necessary.

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

Special Categories of Personal Data

68. The GDPR now refers to sensitive data as “special categories of personal data” (Article 9). These Special categories of data are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Health Data;
- Sexual life / sexual orientation;
- Genetic data – introduced under GDPR;
- Biometric data – introduced under GDPR.

Policy Details

69. 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.

70. Similar considerations apply to personal information concerning other individuals, such as staff. Particular care must be taken to avoid inadvertent or accidental disclosure.

71. 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.

72. Unauthorised staff include those who are not involved in either the clinical care of the service user ort the associated administration processes.

73. 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)

74. 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.

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

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

Disclosing Information

77. The Confidentiality: NHS Code of Practice and the HSCIC Guide to Confidentiality in Health and Social Care provides advice on using and disclosing confidential service user information and has models for confidentiality decisions and all staff must adhere to this guidance.

78. 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.

79. Consent of the individual 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.

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

    - In order to prevent abuse or serious harm to others;

- 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.

81. All individuals must:

- Exercise all due care and diligence to prevent unauthorised disclosure of confidential information as this may lead to disciplinary action;

- Ensure the physical security of all confidential documents, including storage of files on PCs.

82. Any individual has the right to request to see the information an organisation holds about them. This is called a Subject Access request. Any individual making such a request must do so in writing. Contact the Governance Team if you encounter anyone asking for their personal information.

Personal Information

83. In keeping with good Human Resources practice, the CCG retains and processes personal data and special categories of data on its employees for example in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring, for the prevention of fraud or other illegal activities.

84. 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 statutory functions.

85. 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 the Human Resources Team.

Equality, Diversity & Human Rights Impact Assessment

86. The CCG is committed to promoting Equality, Diversity Strategy 2013-2016.

87. It is important to address, through consultation, the diverse needs of our community, patients, their carers and our staff. This will be achieved by working to the values and principles set out in the CCG's Equality, Diversity and Human Rights Strategic Framework.

88. To enable the CCG to meet its legislative duties and regulatory guidance, all new and revised procedural documents, services and functions are to undertake an impact assessment to ensure that everyone has equality of access, opportunity and outcomes regarding the activities. Contact the Governance Team for support to

complete an initial assessment. Upon completion of the assessment, Governance will assign a unique EqIA Registration Number. The CCG undertakes Equality Impact Assessments to ensure that its activities do not discriminate on the grounds of:

- Age;
- Disability;
- Gender reassignment;
- Marriage and civil partnership;
- Pregnancy and Maternity;
- Race;
- Religion or belief;
- Sex;
- Sexual orientation.

89. Before any committee, group or forum validate a strategy, policy or procedural document an EqIA Registration Number will be required.

    This policy has been impact assessed EqIA number 16/13.

Consultation & Approval Process

Consultation

90. In the production of effective strategy and policy documents consultation is vital. The expert group or author should give consideration at an early stage as to where the document will need to be consulted, for example, Information Governance Group.

91. All procedural documents must give consideration to the needs of all potential users and stakeholders. The needs of all equalities categories agreed within the CCG Equality & Diversity Strategy must be addressed.

92. All procedural documents must be developed by local or CCG wide expert groups or personnel. The contributors must be identified within the procedural document.

93. All strategies and policies directly impacting on staff terms and conditions or work practices should be referred to staff side representatives. All staff side issues should be properly consulted with the appropriate personnel.

94. All procedural documents must protect the confidentiality, integrity and accessibilities of information. The CCG Information Governance Team can advise on this. Documents can be referred to them for advice via the Governance Team.

Approval

95. The approval pathway for all procedural documents must be clearly noted on the document control page.

96. Draft strategies and polices should be reviewed by the originating expert group where appropriate. They should then be approved by the relevant committee of the Governing Body for onward approval by the Governing Body.

97. Responsibility for the content, review and distribution of a procedural document lies with the expert group or author responsible for writing it. The most appropriate group or author must be identified and agreed at the outset. This group or author must ensure that the document is aligned with any external standards or accreditation requirements, for example, National Institute for Health and Care Excellence.

98. All procedural documents must contain details on review and revision arrangements including date of review and responsibilities.

99. Strategies and policies can have a reference number which is reference specific. See below for example referencing pre-fixes. To avoid duplication contact the Governance Team before referencing. A unique document number will be applied when the policy is added to the SharePoint, the document number is used for archiving purposes and will remain the same for each subsequent version.

Policy Type	**Prefix Code**
Clinical	CL
Corporate Governance	CG
Finance	FI
Human Resources	HR
IM&T	IT

100. The policy must be referenced to best practice, professional standards and current legislation.

101. A record must be kept within Governance of strategy and policy distribution in order that outdated strategies and policies can be withdrawn and archived as required. Once approved the document should be submitted to the Governance Team to be placed on SharePoint.

Dissemination & Implementation

102. Dissemination: Following approval of strategies, policies and procedural documents it is imperative that all employees and other stakeholders who will be affected by the documents are proactively informed and made aware of any changes in practice that will result. All approved documents will be posted on SharePoint and the CCG's website where appropriate.

103. Implementation: Awareness will be raised regarding the changes to or introduction of this policy via the Governing Body, Committee and Team meetings.

Monitoring Compliance of Procedural Documents

104. The Assistant Director of Governance is responsible for monitoring compliance with the Document Control Policy. This will be completed on an annual basis and reported to the Corporate Governance Committee. The following will be monitored for compliance:

    - Approval processes for strategies and policies;
    - Is there a minute detailing the approval at the appropriate committee and Governing Body?

105. Document and archiving control for strategies and policies:

    - Is the document control page correctly completed including incremental version number?
    - Is this document on SharePoint in PDF format?
    - Is the previous version held on the Governance directorate archive?
    - Does the document meet the standard style and format criteria?

Standards & Key Performance Indicators KPIs

106. This policy will be reviewed yearly or when there are significant changes in the policy.

107. This policy will be monitored for effectiveness by self-assessment against any external accreditation that is applicable and may be subject to review by internal audit.

References & Bibliography

- Data Protection Act 2018
- General Data Protection Regulation 2016
- Human Rights Act 1998
- Freedom of Information Act 2000
- Thefts Act (191968 and 1978)
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act (1988);
- Computer Misuse Act 1990
- Trademarks Act 1994
- Terrorism Act
- Proceeds of Crime Act (2002)
- Money Laundering Regulations 2007
- Criminal Justice and Immigration Act 2008
- Environmental Information Regulations 2004
- Access to Health Records Act 1990
- Digital Economy Act 2017 (Charges and Information) Regulations 2018
- Human Rights Act 1998
- Health & Social Care Act 2012
- Care Act 2014
- Children's Act
- Department of Health's "Confidentiality: NHS Code of Practice" including supplementary guidance "Public Interest Disclosures"
- The Public Interest Disclosure Act 1998
- Code of Practice on Confidential Information https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/code-of-practice-on-confidential-information
- A Guide to Confidentiality in Health & Social Care: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care
- The Social Care Record Guarantee for England
- The NHS Care Record Guarantee for England
- GMC Guidance on Confidentiality: https://www.gmc-uk.org/-/media/documents/confidentiality-good-practice-in-

handling-patient-information---english-0417_pdf-70080105.pdf

- BMA guidance on confidentiality: https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records
- The Caldicott Guardian Manual 2017**:** https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf
- NHS Information Risk Management**:** https://www.igt.hscic.gov.uk/KnowledgeBaseNew/DH_NHS%20IG%20-%20Information%20Risk%20Management%20Guidance.pdf
- Records Management NHS Code of Practice for Health & Social Care 2016: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016
- Data Security and Protection Toolkit (DSPT)
- The Report on the Review of patient-identifiable information (alternative title "The Caldicott Report") and the 'Information: To share or not to share? The Information Governance Review (also known as the Caldicott 2 Review)
- National Data Guardian "Review of Data Security Consent and Opt Outs" July 2016 (also known as Caldicott 3)
- Government Response "Your Data, Better Security, Better Choice, Better Care" July 2017
- Department of Health "2017/18 Data security and protection for health and Social care organisations.
- IGA Guidance: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga
- ICO Guidance : https://ico.org.uk/

Associated CCG Documents

- Disciplinary Policy and Procedure
- Records Management Policy
- Data Security Handbook for CCG Staff
- Data Security Training Needs Analysis