Data Protection and Confidentiality Policy
October 2019

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

Name of Policy:	Data Protection and Confidentiality Policy
Date Issued:	January 2020
Date to be reviewed:	2 years from approval date

Policy Title:	Data Protection and Confidentiality Policy
Supersedes: (Please List)	Data Protection and Confidentiality Policy v0.1, Data Protection and Confidentiality Policy v0.2 and Data Protection and Confidentiality Policy v1.0
Description of Amendment(s):	Addition of Caldicott2 Requirements, in respect of information sharing arrangements and patient information leaflets. Addition of HSCIC Guidance in respect of Confidentiality and Handling Confidential Information. Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation). Changes to principles Guidance on information sharing Breach Reporting Responsibilities Definition of consent
This policy will impact on:	All Staff
Policy Area:	Information Governance
Version No:	2.0
Author:	Humber IG Team
Effective Date:	January 2020
Review Date:	October 2021
Equality Impact Assessment Date:	October 2019

APPROVAL RECORD		**Date:**
	Integrated Audit and Governance Committee	January 2020
Consultation:	Information Governance Steering Group / Relevant Others	October 2019

CONTENTS

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by and Date
0.1	Chris Wallace	First draft for comments	NR
0.2	Barry Jackson	Small amendments	NR
1.0	John Johnson	Addition of Privacy and Electronic communications regulations	NR
1. 1	Helen Sanderson	Addition of HSCIC Guidance and Caldicott 2 requirements	Audit Committee
1.2	Mark Culling	Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).	Integrated Audit and Governance Committee November 2017
2.0	Hayley Gillingwater	Amendments to reflect Data Protection Act 2018 and GDPR Changes to principles Guidance on information sharing Breach Reporting Responsibilities Definition of consent	Integrated Audit and Governance Committee – January 2020

1. INTRODUCTION

1.1. The Hull Clinical Commissioning Group (from this point on known as the CCG) as part of NHS England, a public body, has a statutory duty to safeguard the confidential information it holds. The principle of this policy is that no individual or company working for or with the CCG shall misuse any information it processes or comes into contact with, or allow others to do so. It is also required that all individuals or companies working for or on behalf of the CCG implements appropriate information security to protect the information they process and hold in line with legal obligations and NHS requirements.

1.2. 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 and firm to which this policy applies shall not at any time during the period they work for or provide services to the CCG or at any time after its termination, disclose confidential information that is held or processed by or on behalf of the CCG.

1.3 All staff working in the CCG are bound by a legal 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 within the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), and for health and other professionals, through their own professions Codes of Conduct.

1.4. The CCG places great emphasis on the need for the strictest confidentiality in respect of person identifiable and sensitive data. This applies to manual and computer records and conversations about service user's treatments. Everyone working for the CCG is under a legal duty to keep service user's information, held in whatever form, confidential. Service users who feel that confidence has been breached may issue a complaint under the CCG complaints procedure or they could take legal action.

1.5. Confidentiality should only be breached in exceptional circumstances and with appropriate justification and this must be fully documented.

1.6. 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; and
- understand their rights to access information held about them.

2. SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, volunteers and others undertaking work on behalf of the CCG etc

2.1. 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, service users, 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;
- finance/budget planning/business cases;
- sources of supply and costs of equipment and/or software;
- prospective business opportunities in general;
- computer programs and/or software adapted or used;
- corporate or personnel information; and
- Contractual and confidential supplier information. This is irrespective of whether the material is marked as confidential or not.

3. POLICY PURPOSE AND AIMS

The aims of this policy are:

- to safeguard all confidential information held and processed by the CCG;
- to ensure the CCG has identified a legal basis for holding and processing the specified information;
- to complete Data Protection Impact Assessments on all new ways of processing personal identifiable information;
- to ensure appropriate information sharing agreements are in place for information sharing;
- to provide guidelines in relation to direct marketing regulations
- 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 make all staff aware they are subject to the following legislation:

    - Access to Health Records Act 1990
    - Access to Medical Reports Act 1988
    - Caldicott Committee Report of the Review of Patient-Identifiable

Information 1997
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Data Protection Act 2018
- General Data Protection Regulation
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Human Rights Act 1998
- Gender Recognition Act 2004
- Public Interest Disclosure Act 2013
- Regulation of Investigatory Powers Act 2000
- Re-use of Public Information Regulations 2005
- The Health and Social Care Act 2012
- The Care Act 2014
- Caldicott Review 2012
- The Health and Social Care (Safety and Quality) Act 2015

Data Protection Act 2018:

3.1 The Data Protection Act protects the use of information that identifies individuals (Service users and staff). The purpose of the Data Protection Act is to ensure that the principles of Data Protection are maintained at every stage of information processing, when information is Held, Obtained, Recorded, Used or Shared (HORUS Model).

3.2 Staff must follow the Data Protection principles as outlined below:

- Personal data shall be processed lawfully, fairly and in a transparent manner;
- Personal data shall be obtained for one or more specified and lawful purposes;
- Personal data shall be adequate, relevant and limited to what is necessary;
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of data subjects.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data.
- 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

3.3 The Data Protection Act and GDPR applies to all personally identifiable information regardless of the form in which it was held, for example; information held within computer databases; videos and other automated media; personnel and payroll records; medical records; manual files; microfiche/film; pathology results; x-rays etc.

3.4 The Data Protection Act and GDPR only applies to living individuals, however, the Common Law Duty of Confidentiality extends beyond death and we therefore respect the rights of the deceased in the event of processing a deceased person's personal information. .

3.5 The Data Protection Act dictates that information must only be disclosed on a need-to-know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner. Staff must not disclose information outside legitimate reasons for disclosure.

3.6 Any intentional unauthorised disclosure of information by a member of staff will be considered a disciplinary offence.

3.7 The organisation registers the data it holds with the Information Commissioner's Office, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. The organisation complies with the principles of good practice.

4. General Data Protection Regulation (GDPR)

4.1 The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK. It sets out the key principles, rights and obligations for most processing of personal data.

4.2 Under the GDPR the data protection principles set out the main responsibilities for organisations and are similar to those of the Data Protection Act, with added detail at certain points and a new accountability requirement. There are 7 principles under Article 5 of the GDPR. Article 5 does not have principles relating to individuals' rights or overseas transfers of personal data as these are specifically addressed in separate articles within the GDPR (Chapter 3 and 4 respectively). The 7 principles are outlined below:

4.3

- Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- Personal data must be 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;
- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Personal data must be 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;
- Personal data must be 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;

- Personal data must be 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.

4.4 The most significant addition is the accountability principle. The GDPR requires organisations to show **how** they comply with the above principles – for example by documenting the decisions taken about a processing activity.

4.5 Under GDPR organisations must be able to demonstrate compliance with the requirements of the Regulation at any time.

4.6 Direct Marketing (Privacy and Electronic Communications Regulations)

The Privacy and Electronic Communications Regulations (PECR) set out detailed rules and legal requirements in a number of areas that apply to direct marketing of services and products. The marketing rules apply if you are sending marketing and advertising by electronic means, such as by telephone, email, text, picture or video message, or by using an automated calling system.

The relationship between PECR and the Data Protection Act is a complex one and staff who intend to carry out marketing activities on behalf of the organisation need to be aware of these regulations. Guidance on this is attached with a link to the Information Commissioner's Office and the regulations. See Privacy and Electronic Communications Regulations attached at Appendix 1.

4.7 Conduct

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 by an authorised disclosure for an authorised purpose by the individual or anyone else employed or engaged by the CCG; and/or
- has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure by the individual; 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 regard to the provisions of that Act.

NB/ Disclosures should be in accordance with a relevant information sharing agreement, unless the disclosure is required by law, including under the Public

Interest Disclosure Act 1998. The HSCIC have published a Code of Practice on confidential information and A Guide to Confidentiality in Health and Social Care which give comprehensive guidance in handling and sharing confidential information for different purposes; 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

All individuals must:

- 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 and any mobile equipment. Confidential information must never be left unattended and should be secure when not in use;
- password protect all magnetic media
- passwords must not be disclosed to anyone including colleagues.
- Only use officially issued and fully encrypted mobile equipment in line with the mobile/agile working standard.
- Individuals must implement appropriate information security and safe haven procedures to protect the information they hold and process

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

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

4.8 The duty of confidence

- 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.
- Everyone working for or with the NHS records 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.
- The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.
- 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.

- 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).
- 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.
- Service users are entitled to object to the use of their personal health data for purposes other than their immediate care.
- The duty of confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals.

4.9 What is personal information?

- Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.
- Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary.
- 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.
- If it is not possible to use anonymised data, psuedonymised data should be considered, (data with identifiers removed). This can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data
- Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.
- Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive or special category personal information regarding race, health, sexuality, etc.
- 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.

4.10 Disclosing information

- The HSCIC Code of Practice on Confidential Information and The Guide to Confidentiality in Health and Social Care Services provide advice on using and disclosing confidential service user information and have models for confidentiality decisions and all staff should adhere to this guidance.
- 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.
- The CCG will inform service users, staff and any other data subject why, how and for what purpose personal information is collected, recorded and processed by means of a privacy notice on the CCG website and where necessary service user information leaflets.
- 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.
- 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.
- Where information is required by the police, this must be in line with the Data Protection Act section 29, and staff should consult the Information Governance, Security and Compliance Manager. Decisions on whether to disclose information or not must be recorded.

4.11 Personnel information

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 “special categories of personal data” (as defined by Article 9 of the 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.

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

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 is or may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the Head of Human Resources.

4.12 Media enquiries

All requests for information by the media, other than those made under the Freedom of Information (FOI) Act, must be referred to the Communications and Engagement Team.

4.13 Termination or expiry of a contract with the CCG

On leaving or termination of a contract with the CCG any equipment, copies of software, documents or correspondence, diaries, documents, plans, specifications or any other information relevant to the CCG (whether or not prepared or produced by the individual) must be returned to the CCG's possession and under no circumstances must the leaver take this information with them. All individuals that have left the CCG are bound by the Confidentiality Policy that was in publication at the time of their departure. Line Managers are responsible for ensuring the leavers' process has been correctly followed and that access to all systems and accounts has been revoked and all equipment returned upon termination of an employment contract.

4.14 Awareness and Compliance

It is important to the CCG to protect its legitimate business interests and in particular it's confidential information. Breaches of confidentiality, of any sort, including breach of this policy will be regarded as serious misconduct and may result in:

- dismissal;
- termination of secondment for secondees and a request for their employer to apply their internal disciplinary procedures;
- termination of contracts for interim resources, temporary workers, agency workers and/or contractors; and
- legal action being taken against the discloser and/or any other third party.

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 HR Directorate.

The CCG must report all data breaches that pose a high risk to the rights and freedoms of individuals to the Information Commissioner's Office within 72 hours. To enable the CCG to meet this timescale all data breaches must be reported via the Datix incident reporting system at the earliest opportunity, in order for the Information Governance Team to assess the breach and take appropriate action.

Everyone in the CCG must be aware of the importance of confidentiality. All staff need to be aware of their responsibilities for safeguarding service user confidentiality and keeping information secure.

The duty of confidentiality is written into employment contracts. Breaches of

confidentiality are a serious matter. A breach of confidentiality of information gained, whether directly or indirectly, in the course of duty is a disciplinary offence which could result in dismissal and/ or prosecution. No employee shall knowingly misuse any information or allow others to do so.

It is a disciplinary offence to access records/ information that you have no legitimate reason to view this includes, records about yourself, your family, friends, neighbours, acquaintances. If you do not have a legitimate reason to access, do not browse. Remember all transactions are auditable.

4.15 Rights of the Individual

4.16 Within the Data Protection Act (and GDPR) the individual to whom information relates is referred to as the 'Data Subject'. The Data Subject has the following rights through the Data Protection Act:

- The right to see information that is recorded about them and to make amendments should they not agree with the content. Any amendments should be agreed with the clinician who completed the record. Amendments are only made if information is factually incorrect. The organisation ensures Access to Health Records Procedures are maintained.
- The Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased service user's records.
- The right to prevent processing likely to cause harm or distress
- Individuals can prevent processing (can restrict the uses that their information is put to), if this is likely to cause harm or distress for example information sharing with insurers.
- The right to prevent processing for the purposes of direct marketing
- Under the Act, a data subject can prevent processing of their information, such as asking for addresses / telephone numbers to be deleted from marketing lists.
- The right to have a say in any automated decision making.
- Please Note: The organisation does not undertake automated decision-making.
- The right to take action for compensation if the individual suffers damage.
- If an individual suffers damage as a result of the disclosure of information, for example comments made about treatment undertaken, then the data subject may bring an action against the person who made the disclosure.
- The right to take action to rectify, block, erase or destroy inaccurate data
- If a data subject does not agree with the content of a record, they can ask that this be amended with the agreement of the clinician who completed the record. It is ONLY for a court to decide that a record can be deleted in this case. Amendments are only made if information is factually incorrect..
- The right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

If the Data Subject feels that the Act has been contravened in respect of their rights, they can make a request to the Information Commissioner for

this to be reviewed.

Under GDPR the Data Subject has the following rights:

- The right to be informed (through the use of privacy notices)
- The right of access (confirmation that the data subject's information is being processed, access to their personal information, other supplementary information relating to the use of the personal information, who it is shared with, the retention periods and information on how to complain about the use of the data)
- The right to rectification (if information is inaccurate or incomplete)
- The right to erasure (subject to conditions)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

4.17 Consent to process service users' identifiable health or care information for anything other than direct care must be sought from the data subject.

Valid consent is central in all forms of healthcare, from using information to undertaking major surgery.

"Consent" is a service user's agreement for a process to be undertaken, whether this be the sharing of information or the provision of care. For the consent to be valid, the service user must:

- be competent to take the particular decision;
- have received sufficient information to take it; and
- not be acting under duress.

Consent can be written, verbal, or implied (implied consent can only be used in the context of the delivery of direct care by a member of the care team).

Where an adult service user lacks the mental capacity (either temporarily or permanently) to give or withhold consent for themselves, no-one else can give consent on their behalf**.** Service Users can make advance statements and/or directives regarding giving or withholding consent should they lack the mental capacity (either temporarily or permanently) at some point in the future to do so.

When seeking consent on behalf of children, a child's capacity to decide whether to consent to or refuse proposed investigation must be assessed prior to consent being sought. In general, a competent child will be able to understand the nature, purpose and possible consequences of the proposed investigation or treatment, as well as the consequences of non-treatment. The following should be considered in this instance:

- at age 16 a young person can be treated as an adult and can be presumed to have capacity to decide;

- under age 16 children may have capacity to decide, depending on their ability to understand what is involved (according to Fraser Ruling, (formerly Gillick Competency), whereby a child under 16 is of sufficient maturity to understand the treatment and risks and is able to make a valid consent to treat).

Explicit consent must always be sought from the service user in order to use their personal information in ways that do not directly contribute to or support the delivery of their care.

5.0 IMPACT ANALYSIS

5.1 Equality

This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

A Government equality impact assessment of the Data Protection Bill in 2017, cites an overall positive impact. More information given in the Equality Impact Assessment below.

5.2 Bribery Act 2010

NHS Hull Clinical Commissioning Group has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010.

The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf.

If you require assistance in determining the implications of the Bribery Act please contact the Local Counter Fraud Specialist on telephone number 01482 866800 or

email at nikki.cooper1@nhs.net.

Due consideration has been given to the Bribery Act 2010 in the development of this policy (or review, as appropriate) of this policy document and no specific risks were identified.

6. NHS CONSTITUTION

6.1 The CCG is committed to: Designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantaged.

6.2 This Policy supports the NHS Constitution as follows:

The NHS aspires to the highest standards of excellence and professionalism in the provision of high-quality care that is safe, effective and focused on patient experience; in the planning and delivery of the clinical and other services it provides; in the people it employs and the education, training and development they receive; in the leadership and management of its organisations; and through its commitment to innovation and to the promotion and conduct of research to improve the current and future health and care of the population.

7. ROLES / RESPONSIBILITIES / DUTIES

Management Responsibilities for Data Protection

7.1 The **Chief Finance Officer** has overall responsibility for the Data Protection Act within the organisation, who is also the nominated Senior Information Risk Officer (SIRO). The implementation of, and compliance with this Act is delegated to other designated personnel as appropriate.

7.1.2 **The Senior Information Risk Owner (SIRO)** role includes:

owning of the organisation's Information Risk Policy and risk assessment process and acting as an advocate for information risk on the Governing Body

owning of risk assessment processes, including the review of the annual information risk assessment and agree action in respect of these risks.

ensuring that the organisation's approach to information risk is effective in terms of resources, commitment and execution and that this is communicated to all staff.

7.1 **Data Protection Officer** – under GDPR public authorities or organisations who carry out large scale processing of sensitive data must appoint a Data Protection Officer. The role of Data Protection Officer is to facilitate the CCG's compliance with GDPR and will:

- Monitor CCG compliance with the GDPR
- Provide advice and assistance with regards to the completion of Data Protection Impact Assessments

- Act as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to GDPR and the protection of personal information
- Assist in implementing essential elements of the GDPR such as the principles of data processing, data subjects' rights, data protection impact assessments, records of processing activities, security of processing and notification and communication of data breaches

7.5 The **Caldicott Guardian** is responsible for overseeing and advising on issues of service user confidentiality for the CCG. Every NHS organisation is required to appoint a Senior Health Professional as Caldicott Guardian to oversee the processing of service user's identifiable information. The **Director of Quality and Clinical Governance** is the CCG's Caldicott Guardian. This is to ensure the organisation is compliant with the Caldicott Principles governing the use of identifiable information. These principles are as follows:

- Formal justification of purpose
- Information only processed when necessary
- Only the minimum information necessary
- Need-to-know access controls
- All Users must understand their responsibilities
- Comply with and understand the law
- the duty to share information can be as important as the duty to protect patient confidentiality

All service users' information processed must comply with the above principles.

7.6 All service users' information that is processed must have agreement by the Caldicott Guardian that the process follows the above principles.

7.7 If any member of staff or department has a requirement to process identifiable information that does not have agreement from the Caldicott Guardian, this must be obtained.

7.8 The Caldicott Guardian is also responsible for:

- The protection and confidentiality of patient-identifiable information, both within the organisation and when sharing it with other organisations
- Agreeing levels of access to the organisation's patient information systems.
- ensure the confidentiality and data protection work programme is successfully coordinated and implemented;
- ensure compliance with the principles contained within the Confidentiality: NHS Code of Practice and that staff are made aware of individual responsibilities through policy, procedure and training;

7.9 . All information management and technology security (Cyber) incidents and weaknesses must be reported immediately in line with the CCG Incident Reporting Policy.

7.10 Incidents that present an immediate risk to the CCG such as viruses should also be reported to the IT Service Desk immediately.

7.11 Information Security Incidents, especially those involving the loss of sensitive or confidential data, or any incident involving unencrypted portable devices may need to be reported as a Serious Incident and/ or to the Information Commissioner via the Information Governance Toolkit reporting system. See the Incident Reporting policy for more details.

7.12 There is a legal requirement to report any such serious incidents to the authorities within 72 hours.

7.13 All staff undertake appropriate annual data security training, renamed "Data Security Awareness Level 1" to reflect Data Security Standard 3 in the Caldicott 3 Review, and pass a mandatory test.

7.14 The CCG obtains regular assurance from Core IT providers that CareCert Alerts are being acted upon and are being addressed appropriately. CareCert informs organisations about cyber security vulnerabilities, mitigating risks, and reacting to cyber security threats and attacks.

7.15 Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information. They are also responsible for monitoring compliance with this guideline e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

7.16 Line Managers are responsible for ensuring that access to the folders held on the Y-Drive is appropriately allocated. Staff should only have access to folders necessary for their job roles; if staff become aware that they have access to an area that is not required they should inform their Line Manager so that access can be restricted.

7.17 Staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment with the CCG and this extends after they have left the employ of the CCG.

7.18 Individual staff members are personally responsible for any decision to pass on information that they may make.

7.19. All staff are responsible for adhering to the Caldicott principles, the Data Protection Act, and the Confidentiality Code of Conduct.

7.20. 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 (e.g. team brief/team meetings);
- CCG Website;

7.21 All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided within the first year of employment and then updated as appropriate in accordance with the Statutory and Mandatory Training Standard and Information Governance Training Needs Analysis.

7.22 The CCG must ensure that all contractors and supporting organisations are working to documented contracts or service level agreements that detail their responsibilities in respect of information governance and security, and confidentiality and data protection. This includes the completion of the Data Security & Protection Toolkit to a satisfactory standard.

8. IMPLEMENTATION

The policy will be disseminated by being made available on the CCG website and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

9. TRAINING AND AWARENESS

Staff will be made aware of the policy via the CCG's website and staff communications.

10. MONITORING AND EFFECTIVESNESS

10.1. Performance against the Data Securityand& Protection Toolkit will be reviewed on an annual basis and used to inform the development of future procedural documents.

10.2. This policy will be reviewed every two years, and in accordance with the following on an as and when required basis:

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

10.3. Records Management, Retention and Disposal

10.3.1. A records management system must be implemented to ensure that all

records are maintained in accordance with the Data Protection Act and Caldicott Principles (See Annexes A&B), and the NHS Records Management, Code of Practice.

10.3.2 The records management systems must include appropriate controls to protect information from unauthorised access, theft or loss, and inappropriate disclosure of person identifiable or corporately confidential information.
10.3.3 A system of timely housekeeping must be implemented and include secure methods of destruction for records that have reached their retention period and been assessed as not to be retained for permanent preservation.

10.4. Complaints The CCG will implement a complaints procedure to deal with complaints in connection with the Data Protection Act and breaches of confidentiality. If the complainant is not satisfied with the investigation and outcome of their complaint they should be advised of their right to contact the Information Commissioners Office.

11. POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

11. REFERENCES

Privacy and Electronic Privacy Regulations Access to Health Records Act 1990
Access to Medical Reports Act 1988
Caldicott Committee Report of the Review of Patient-Identifiable Information 1997
Common Law Duty of Confidentiality
Computer Misuse Act 1990
Crime and Disorder Act 1998
Criminal Justice Act 2003
Environmental Information Regulations 2004
Freedom of Information Act 2000
Human Rights Act 1998
Public Interest Disclosure Act 2013
Regulation of Investigatory Powers Act 2000
Re-use of Public Information Regulations 2005
The Health and Social Care Act 2012
The Care Act 2014
Caldicott Review 2012
The Health and Social Care (Safety and Quality) Act 2015
Data Protection Act 2018 (DPA)
General Data Protection Regulation (GDPR)

Appendix 1
The Data Protection Act and Direct Marketing

This Appendix is to give an overview of the subject of direct marketing in data protection from guidance published by The Information Commissioner's Office (ICO).
The ICO has received a large number of complaints about unwanted marketing calls and texts. Their focus is on reducing the number of complaints by taking systematic enforcement action.
The subject of direct marketing and how it relates to data protection is complex, therefore this guidance cannot cover the subject in its entirety or great detail enough to ensure compliance. Staff should use the link provided at the end of this document to access the guidance published by the Information Commissioner's Office on direct marketing for the more comprehensive information about marketing & legal requirements.

Direct Marketing Definition
The Data Protection Act 2018 (DPA) incorporating the requirements of the General Data Protection Regulation (GDPR), defines direct marketing as:
"the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".
The above definition applies to the Privacy & Electronic Communications Regulations (PECR). This is because although direct marketing is not specifically defined in PECR, regulation 2 of PECR states that any expressions that are not defined in PECR will have the same meaning as defined in DPA.
This definition covers any advertising or marketing material, not just commercial marketing. All promotional material falls within this definition, including material promoting the aims of not-for-profit organisations, even if that is not the main purpose of the material published.
The definition also covers any means of communication, it is not limited to traditional forms of marketing such as telesales or mailshots, and can extend to online marketing, social networking or other emerging channels of communication.
The key element of the definition is that the material must be directed to particular individuals. Indiscriminate blanket marketing – for example, leaflets delivered to every house in an area, magazine inserts, or adverts shown to every person who views a website – will not therefore fall within this definition of direct marketing.

Legal Framework for Direct Marketing
The Data Protection Act (DPA), General Data Protection Regulation (GDPR) and Privacy & Electronic Communications Regulations (PECR) restrict the way organisations can carry out unsolicited direct marketing (that is, direct marketing that has not specifically been asked for by the intended recipient).

Main Areas of the Data Protection Act / General Data Protection Regulation

In order to understand the requirements of the DPA (and GDPR) there are a number of definitions of terms which are required:

Data Subject:	The person to whom information relates
Data Processor	A person performing processing tasks of the Data Controller
Data Controller:	The person with overall responsibility for

maintaining

the information system, and who has responsibility for compliance to the DPA (or GDPR). A Data Controller is defined as an individual who (either alone or jointly) determines the purposes for which and the manner in which any personal data about an individual are, or are to be, processed

Processing Information: Putting the information collected to a specific use, either compiling a clinic list, or typing clinic letters is an information process. It covers all recording, obtaining, holding, altering, retrieving, destroying, or disclosing data.

Personal Information: Information from which an individual can be identified

Relevant Filing System: Information stored either in alphabetical or other easily accessible form from which individuals can be identified.

Sensitive Information (Special Category Information): Information relating to sex life or sexual orientation, race or ethnic origin, political or Religious or philosophical beliefs, trade union membership, or physical or mental health condition. (Under GDPR the categories of sensitive information are known as Special Categories of data and include the same as those under DPA in addition to genetic data and biometric data for the purpose of uniquely identifying a natural person)

Notification: Advising the Information Commissioner of the extent

and type of information held, and demonstrating compliance to the DPA (and GDPR).

All processing of personal data must comply with the 8 principles of the Data Protection Act (6 principles of GDPR).

GDPR Article 6 Lawful Basis:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary:
    - in relation to a contract which the individual has entered into; or
    - because the individual has asked for something to be done so they

can enter into a contract.

- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition (not available to public bodies under GDPR).

GDPR Article 9:

- The individual whom the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…;
- The processing is necessary to protect the vital interests of:
    - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
    - another person (in a case where the individual's consent has been unreasonably withheld).
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

https://ico.org.uk/for-organisations/guide-to-data-protection/

https://ico.org.uk/for-organisations/data-protection-reform/

Privacy & Electronic Privacy Regulations (PECR)
PECR has been designed to complement the Data Protection Act and set out more detailed privacy rules in relation to the developing area of electronic communications. Regulation 4 of PECR states that nothing contained in those regulations relieves a person from their obligations under the DPA in terms of processing personal data.
Market Research

If an organisation contacts customers to conduct genuine market research (or contracts a research firm to do so), this will not involve the communication of advertising or marketing material, and so the direct marketing rules will not apply. However, organisations conducting market research will still need to comply with other provisions of the DPA, and in particular ensure they process any individually identifiable research data fairly, securely and only for research purposes.
However, an organisation cannot avoid the direct marketing rules by labelling its message as a survey or market research if it is actually trying to sell goods or services, or to collect data to help it (or others) to contact people for marketing purposes at a later date.
If an organisation claims it is simply conducting a survey when its real purpose (or one of its purposes) is to sell goods or services, generate leads, or collect data for marketing purposes, it will be breaching the DPA when it processes the data.

Solicited and unsolicited marketing
There is no restriction on sending solicited marketing – that is, marketing material that the person has specifically requested. PECR rules only apply to 'unsolicited' marketing messages, and the DPA will not prevent an organisation providing information which someone has asked for. So, if someone specifically asks an organisation to send them particular marketing material, it can do so.
If the marketing has not been specifically requested, it will be unsolicited and the PECR rules apply. This is true even if the customer has 'opted in' to receiving marketing from that organisation.
An opt-in means that the customer is happy to receive further marketing in future, and is likely to mean the unsolicited marketing is lawful (see the next section on consent). But it is still unsolicited marketing, which means the PECR rules apply.

Consent

Consent is defined in DPA, and therefore applies to PECR, as:

'a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data.'

Consent is central to the rules on direct marketing. Organisations will generally need an individual's consent before they can send marketing texts, emails or faxes, make calls to a number registered with the TPS, or make any automated marketing calls under PECR. They will also usually need consent to pass customer details on to another organisation under the first data protection principle. If they cannot demonstrate that they had valid consent, they may be subject to enforcement action.
To be valid, consent must be knowingly given, clear and specific. Organisations should keep clear records of what an individual has consented to, and when and how this consent was obtained, so that they can demonstrate compliance in the event of a complaint.
Marketing calls
General rule: screen live calls against the Telephone Preference Service (TPS)
Organisations can make live unsolicited marketing calls, but must not call any number registered with the TPS unless the subscriber (ie the person who gets the telephone bill) has specifically told them that they do not object to their calls. In effect, TPS registration acts as a general opt-out of receiving any marketing calls.
In practice, this means that to comply with PECR, organisations should screen the list of

numbers they intend to call against the TPS.

Business-to-business calls

The same rules apply to marketing calls made to businesses, sole traders and partnerships may register their numbers with the TPS in the same way as individual consumers, while companies and other corporate bodies register with the Corporate Telephone Preference Service (CTPS). So organisations making business-to-business marketing calls will need to screen against both the TPS and CTPS registers.

Marketing texts and emails

General rule: only with consent

Organisations can generally only send marketing texts or emails to individuals (including sole traders and some partnerships) if that person has specifically consented to receiving them. Indirect consent (i.e. consent originally given to a third party) is unlikely to be sufficient. Refer to guidance on consenting considerations.

The same rule applies to any marketing sent by 'electronic mail', which is defined in PECR as:

"any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service".

In other words, the same rules will apply to any electronically stored messages, including email, text, picture, video, voicemail, answerphone and some social networking messages. The rules also still apply to viral marketing – organisations will still need consent even if they do not send the messages themselves, but instead instigate others to send or forward them. Organisations must not disguise or conceal their identity in any marketing texts or emails, and must provide a valid contact address for individuals to opt out or unsubscribe (which would mean consent was withdrawn). It is good practice to allow individuals to reply directly to the message and opt out that way, to provide a clear and operational unsubscribe link in emails or at least to provide a freephone number.

Existing customers: the 'soft opt-in'

Although organisations can generally only send marketing texts and emails with specific consent, there is an exception to this rule for existing customers, known as the 'soft opt-in'. This means organisations can send marketing texts or emails if:

- they have obtained the contact details in the course of a sale (or negotiations for a sale) of a product or service to that person;
- they are only marketing their own similar products or services; and
- they gave the person a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.

The texts or emails must be marketing products or services, which means that the soft opt-in exception can only apply to commercial marketing. Charities, political parties or other not for-profit bodies will not be able to rely on the soft opt-in when sending campaigning texts or emails, even to existing supporters. In other words, texts or emails promoting the aims or ideals of an organisation can only be sent with specific consent.

The right to opt out

Organisations must not send marketing texts or emails to an individual who has said they do not want to receive them. Individuals have a right to opt out of receiving marketing at any time. Organisations must comply with any written objections promptly to comply with

the DPA – but even if there is no written objection, as soon as an individual says they don't want the texts or emails, this will override any existing consent or soft opt-in under PECR and they must stop.

You must not make it difficult to opt out, for example by asking customers to complete a form or confirm in writing. It is good practice to allow the individual to respond directly to the message – in other words, to use the same simple method as required for the soft opt-in. In any event, as soon as a customer has clearly said that they don't want the texts or emails, the organisation must stop, even if the customer hasn't used its preferred method of communication.

Business-to-business texts and emails
These rules on consent, the soft opt-in and the right to opt out do not apply to emails sent to companies and other corporate bodies (e.g. limited liability partnerships, Scottish partnerships, and government bodies). The only requirement is that the sender must identify itself and provide contact details.
However, it serves little purpose to send unsolicited marketing messages to those who have gone to the trouble of saying they do not want to receive them. In addition sole traders and some partnerships do in fact have the same protection as individual customers. If an organisation does not know whether a business customer is a corporate body or not, it cannot be sure which rules apply. Therefore we strongly recommend that organisations respect requests from any business not to email them.
In addition, many employees have personal corporate email addresses to which marketing messages could be sent (e.g. firstname.lastname@org.co.uk), and individual employees will have a right under section 11 of the DPA to stop any marketing being sent to that type of email address.

Other Types of Direct Marketing
The focus of the ICO guidance is on marketing calls and texts (and by extension, emails and other forms of electronic mail). However, PECR also specifically regulate marketing by fax, and the DPA can apply to any other type of direct marketing. These are also covered in more detail in the ICO guidance but in brief, these include:

Marketing Faxes
Organisations must not send marketing faxes to individuals (including sole traders and some partnerships) without their specific consent. See the section above on what counts as consent.
Organisations can send marketing faxes to companies (or other corporate bodies) without consent, but must not fax any number listed on the Fax Preference Service (FPS) unless that company has specifically said that they do not object to those faxes. This means that to comply with PECR, organisations will need to screen the list of numbers they intend to fax against the FPS register.

Marketing Online
Organisations must comply with the DPA if they are targeting online adverts at individual users using their personal data – which might apply if, for example, they display personalised adverts based on browsing history, purchase history, or log-in information.

Marketing Mail
PECR does not cover marketing by mail, but organisations sending marketing mail to named individuals must comply with the DPA. If an organisation knows the name of the person it is mailing, it cannot avoid DPA obligations by simply addressing the mail to 'the

occupier', as it is still processing that individual's personal data behind the scenes.
In essence, the DPA requires that an individual is aware that an organisation has their contact details, and intends to use them for marketing purposes. The organisation must have obtained the address fairly and lawfully. It cannot send marketing mail if the address was originally collected for an entirely different purpose.

Lead Generation and Marketing Lists

Marketing lists can be compiled in different ways, and vary widely in quality. A good marketing list will be up to date, accurate, and reliably record specific consent for marketing. A list like this can be used in compliance with the law and should generate few – if any – complaints. However, other lists may be out of date, inaccurate, and contain details of people who have not consented to their information being used or disclosed for marketing purposes. Using such a list is likely to result in a breach of both the DPA and PECR.

A list might contain data compiled in-house from customer contacts. Or it might be a bought-in list of people an organisation has never dealt with directly. Or it could be a mixture of the two. This is an important distinction, because a list compiled in-house should be more accurate and up to date – and easier to check. Quality issues are harder to identify if lists are bought in. And, for certain types of marketing, the law works differently if people's details were not obtained directly.

Generating Leads

There are a wide range of sources for marketing leads. These might include public directories, previous customers and people who have sent an email, registered on a website, subscribed to offers or alerts, downloaded a mobile app, entered a competition, used a price-comparison site to get a quote, or provided their details in any other way. An organisation may be able to legitimately use these sources, but must ensure that it complies with the DPA – and in particular that it acts fairly and lawfully – whenever and however it collects personal data.

If collecting contact details directly from individuals, an organisation should provide a privacy notice explaining clearly that it intends to use those details for marketing purposes. This should not be hidden away in a dense or lengthy privacy policy or in small print. Organisations must not conceal or misrepresent their purpose (eg as a survey or competition entry) if they also intend to use the details for marketing purposes. And if they intend to sell or disclose the details to other organisations, the privacy notice should make this very clear, and get the person's specific consent for this.

Buying a Marketing List

Organisations buying or renting a marketing list from a list broker or other third party must make rigorous checks to satisfy themselves that the third party obtained the personal data fairly and lawfully, that the individuals understood their details would be passed on for marketing purposes, and that they have the necessary consent.

Organisations should take extra care if using a bought-in list to send marketing texts, emails or automated calls. They must have very specific consent for this type of marketing, and indirect consent (ie consent originally given to another organisation) will not always be enough. Remember also that the 'soft opt-in' exception for email or text marketing cannot apply to contacts on a bought-in list.

ICO PECR guidance can be found at:
http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/direct-marketing-guidance.pdf

Please refer to the EIA Overview & Navigation Guidelines located in *Y:\HULLCCG\Corporate Templates and Forms\Equality and Diversity Information* before completing your EIA)

HR / Corporate Policy Equality Impact Analysis:	
Policy / Project / Function:	Data Protection and Confidentiality Policy 2.0
Date of Analysis:	31/10/2019
Completed by: **(Name and Department)**	Hayley Gillingwater – Senior Information Governance Specialist
What are the aims and intended effects of this policy, project or function?	The overall purpose of the policy is to set out the CCG's approach to Data Protection and Confidentiality within the workplace. The policy will also set out guidance to staff and managers about their responsibilities in relation to Data Protection and Confidentiality.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	No
Please list any other policies that are related to or referred to as part of this analysis	Privacy & Electronic Privacy Regulations Access to Health Records Act 1990 Access to Medical Reports Act 1988 Caldicott Committee Report of the Review of Patient-Identifiable Information 1997 Common Law Duty of Confidentiality Computer Misuse Act 1990 Crime and Disorder Act 1998 Criminal Justice Act 2003 Environmental Information Regulations 2004 Freedom of Information Act 2000

	Human Rights Act 1998 Gender Recognition Act 2004 Public Interest Disclosure Act 2013 Regulation of Investigatory Powers Act 2000 Re-use of Public Information Regulations 2005 The Health and Social Care Act 2012 The Care Act 2014 Caldicott Review 2012 The Health and Social Care (Safety and Quality) Act 2015 Data Protection Act 2018 (DPA) General Data Protection Regulation (GDPR)
Who will the policy, project or function affect?	Employees and the general public
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Consultation on the updated policy has taken place locally.
Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of	The policy does not directly promote inclusivity but provides a framework for the handling of data protection and confidentiality ensuring staff are supported by management and health professionals.

access needs	

Equality Data	
Is any Equality Data available relating to the use or implementation of this policy, project or function? Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *'Equality Groups'.* Examples of *Equality Data* include: (this list is not definitive) 1: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share / represent protected characteristics 4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	Yes ☐ No ☒ x Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact? **Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

Assessing Impact				
Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups? (Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)				
Protected Characteristic:	**Neutral Impact:**	**Positive Impact:**	**Negative Impact:**	**Evidence of impact and, if applicable, justification where a *Genuine Determining Reason*[1] exists (see footnote below – seek further advice in this case)**
It is anticipated that these guidelines will have a positive impact as they support policy writers to complete meaningful EIAs, by providing this template and a range of potential issues to consider across the protected characteristics below. There may of course be other issues relevant to your policy, not listed below, and some of the issues listed below may not be relevant to your policy. Overall impact: An equality impact assessment conducted by the Department for Digital, Culture and Media[2] cites an overall positive equality impact of the new data protection regulations that this policy is based on: *"There is reason to believe that the cross-cutting provisions of the new data protection law will serve to promote equality. For example, data subjects will benefit from strengthened rights to access personal data held about them, and for the first time this must be provided at no charge. Data subjects will continue to benefit from the ability to confirm personal data is accurately recorded, including by correcting inaccurate or outdated information, and backed by increased sanctions and penalties available to the Information Commissioner. There is some anecdotal evidence to suggest that existing data subject access rights have had a positive impact on individuals who believe they may have been discriminated against because it enables them to access information for use in discrimination complaints or litigation (for example discrimination relating to employment, an organisation's decision making process or consumer issues)."*				
Gender	x			This policy applies to all regardless of gender.
Age	x			This policy applies to all regardless of age.
Race / ethnicity / nationality	x			This policy applies to all regardless of race/ethnicity/nationality.

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711171/Equality_Impact_Assessment.pdf

Disability	x			This policy applies to all regardless of disability.
Religion or Belief	x			This policy applies to all regardless of religion or belief.
Sexual Orientation	x			This policy applies to all regardless of sexual orientation.
Pregnancy and Maternity	x			This policy applies to all regardless of pregnancy/ maternity.
Transgender / Gender reassignment	x			This policy applies to all regardless of transgender/ gender reassignment.
Marriage or civil partnership	x			This policy applies to all regardless of marriage or civil partnership.

Action Planning:				
As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?				
Identified Risk:	**Recommended Actions:**	**Responsible Lead:**	**Completion Date:**	**Review Date:**
It is recognised that this Policy is written in English and there is therefore a risk to the staff whose first language is not English for misunderstanding.	The CCGs internal 'portal' and external website signpost individuals to alternative formats such as large print, braille or another language.	CCG Communications	Updating of this facility is ongoing	Next Policy Review November 2021.

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs
I agree / disagree with this assessment / action plan
If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:
 **Signed:**
Date: 19.12.19